PARTNER SOLUTION GUIDE

Wave 6 | August 2012 | 3725-62124-003 Rev A

Polycom® Unified Communications Deployment Guide for Siemens Enterprise Communications® OpenScape® Environments

Polycom® Unified Communications Deployment Guide for Siemens Enterprise Communications OpenScape Environments

Copyright ©2012, Polycom, Inc. All rights reserved.

6001 America Center Drive
San Jose, CA 95002
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

Trademarks

POLYCOM®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided “as is” without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to videodocumentation@polycom.com.

Visit Polycom Support Polycom Strategic Global Partner Solutions for software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

Contents

About This Guide vii

Conventions Used in this Guide vii
Information Elements vii
Typographic Conventions viii

Chapter 1: Introducing Siemens OpenScape Video Solution 1

Before You Begin 1
Required Solution Hardware 1
Hardware and Software Dependencies 2
Finding Help and Support Resources 3

Chapter 2: Understanding the OpenScape Video Solution Features 5

Understanding OpenScape Unified Communications 5
OpenScape UC Services 5
OpenScape UC Devices 5
OpenScape UC Features 6
Integrating OpenScape Video and OpenScape Voice 6
Understanding Mixed-Media Collaboration Sessions 7
Using Interdomain Video 7

Chapter 3: Understanding the OpenScape Video Architecture 9

Physical Layer 9
Session Initiation Protocol (SIP) Layer 10
H.323 DMA System as Gatekeeper 11
Overview of the OpenScape Video Solution 12
Using Non-SIP Components 12
Connecting H.323 Video Endpoints OpenScape Video 12
Connecting non-IP Video Endpoints to OpenScape Video 13

Chapter 4: Understanding OpenScape Video Use Cases 15

Understanding Interdomain Video Solutions 15
Session Border Controller (SBC)-Based Interdomain Video 15
VPN-Based Interdomain Video 16
Gateway-Based Interdomain Video 16
Connecting Multiple On-Site Video Endpoints 18

Connecting Multiple Off-Site Video Endpoints 18
Understanding OpenScape Location and Identity Assurance (LIA) Network Automation Support for Polycom Video Endpoints 19
Understanding Quality of Service 20
Using Virtual MCUs in OpenScape Video 21
Connecting Redundant MCUs Using the Polycom DMA System 21
Use Cases for Resilient Video Conferencing 22
Centralized Conference Resource Management 22
Automatically Routing Around Outages 23

Chapter 5: Configuring Siemens OpenScape Voice 25

Configuring OpenScape Voice Subscriber 25
Configuring OpenScape Voice Endpoints 26

Chapter 6: Integrating Polycom HDX Systems with Siemens OpenScape 29

Configuring Polycom HDX Systems LAN Properties 29
Specifying HDX SIP Settings 34
Specifying H.323 Settings (Optional) 37
Using Polycom's On Demand Conferencing Solution 40

Chapter 7: Integrating Polycom RMX Systems with Siemens OpenScape 41

Defining IP Network Services 41
Setting Mandatory System Flags 42
Creating a Primary Management Network 44
Setting Up a Conferencing Network Service 45
Modifying the Management Network Service 45
Modifying the Network Service 52
Configuring RMX IP Settings 52
Configuring RMX Routers 55
Configuring Gatekeeper Settings 56
Configuring Ports 59
Configuring QoS Settings 60
Configuring the SIP Servers 62
Configuring Security Settings 66
Modifying Ethernet Settings 68
Monitoring the IP Network 71
Using IPv6 Network Addresses for RMX Internal and External Entities 75
RMX Internal Addresses 75
External Entities 75
IPv6 Guidelines 75

Viewing Licensing and System Information 76

Chapter 8: Integrating Polycom VVX Phones with Siemens OpenScape 79

Configuring Polycom VVX 1500 SIP Settings.....79

Chapter 9: Integrating Polycom DMA Systems with Siemens OpenScape..... 83

Configuring the Polycom DMA System SIP Settings.....83

Chapter 10: Known Issues..... 89

About This Guide

Conventions Used in this Guide

This user guide contains terms, graphical elements, and a few typographic conventions. Familiarizing yourself with these terms, elements, and conventions will help you perform phone tasks.

Information Elements

The following icons are used to alert you to various types of important information in this guide:

Icons Used in this Guide

Name	*Icon*	*Description*
Note		The *Note* icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.
Administrator Tip		The *Administrator Tip* icon highlights techniques, shortcuts, or productivity related tips.
Caution		The *Caution* icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.
Warning		The *Warning* icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone or network performance.
Web Info		The *Web Info* icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.
Timesaver		The *Timesaver* icon highlights a faster or alternative method for accomplishing a method or operation.
Power Tip		The *Power Tip* icon faster, alternative procedures for advanced administrators already familiar with the techniques being discussed.
Troubleshooting		The *Troubleshooting* icon highlights information that may help you solve a relevant problem or to refer you to other relevant troubleshooting resources.
Settings		The *Settings* icon highlights settings you may need to choose for a specific behavior, to enable a specific feature, or to access customization options.

Typographic Conventions

A few typographic conventions, listed next, are used in this guide to distinguish types of in-text information.

Typographic Conventions

Convention	*Description*
Bold	Highlights interface items such as menus, soft keys, file names, and directories. Also used to represent menu selections and text entry to the phone.
Italics	Used to emphasize text, to show example values or inputs, and to show titles of reference documents available from the Polycom Support Web site and other reference sites.
Underlined Blue	Used for URL links to external Web pages or documents. If you click on text in this style, you will be linked to an external document or Web page.
Blue Text	Used for cross references to other sections within this document. If you click on text in this style, you will be taken to another part of this document.
`Fixed-width-font`	Used for code fragments and parameter names.

Chapter 1: Introducing Siemens OpenScape Video Solution

This partner solution guide explains how to integrate Siemens OpenScape® Video V6 with Polycom Unified Communications (UC). Siemens OpenScape Video includes OpenScape Voice, part of Siemens Enterprise Communications, and combines high-definition (HD) video, voice, and web collaboration tools into a single unified communications and collaboration (UCC) environment. This partner solution guide is intended for administrators integrating Siemens with Polycom products and for support personnel working with customers to set up the solution described in this guide.

Siemens OpenScape Video and OpenScape® Voice are session initiation protocol (SIP)-based communications technologies that integrate with your existing video, voice, and web communications applications and enable you to unify your communications environment. OpenScape Video provides easy transition from H.323 to SIP, enabling you to connect video endpoints using H.323 or SIP through IP-to-IP gateways or session border controllers (SBCs). This partner solution guide uses the Acme Packet Net-Net SBC in UC architecture examples and use cases. You can use OpenScape Video to set up video conferences with a *virtual* multipoint control unit (MCU) that consists of multiple physical MCUs and a mechanism that balances resource use and controls switchover in the event of outages.

Before You Begin

Administrators require the following to perform the steps in this partner solution guide:

- Previous knowledge of, and experience with, the Siemens OpenScape components
- Access to Siemens OpenScape product documentation and relevant software
- Knowledge of and experience with Polycom CMA systems, Polycom DMA systems, Polycom HDX systems, Polycom RMX systems, Polycom VVX 1500 phones, and Polycom RPX, ATX, and OTX components
- Access to Polycom product documentation and relevant software

Required Solution Hardware

To begin setting up Siemens OpenScape Video for integration with Polycom products, you need the following Siemens and Polycom hardware components:

Siemens

This partner solution guide requires you to have the following Siemens hardware components. You can operate the hardware components on a single server or each on a separate server:

- OpenScape Voice switch
- OpenScape UC application
- OpenScape Media Server
- (Optional) Siemens OpenStage 5/15/20/40/60 and OpenStage 80 phones

Note: Understanding Two OpenStage Software Versions

Note that there are two OpenStage software versions. OpenStage phones 5, 15, 20, and 40 use a software version that is different from OpenStage phones 60 and 80.

Polycom

The following is a list of Polycom products you can use with the solution provided in this partner solution guide. This solution requires either a Polycom HDX system or a VVX 1500. All other products listed are optional and can be integrated with this solution. You can operate the hardware components on a single server or each on a separate server:

- (Required) Polycom® HDX® Series Systems
- Polycom® Converged Management Application™ (CMA®) 5000 Server
- Polycom® Distributed Media Application™ (DMA™) 7000 Server
- Polycom® RMX® 1500/2000/4000
- Polycom® VVX® 1500 Business Media Phone
- Polycom® RealPresence™ Experience, (RPX™), Polycom® Architected Telepresence Experience™ (ATX™), and Polycom® Open Telepresence Experience™ (OTX™)

Hardware and Software Dependencies

The following tables, Table 1-1 and Table 1-2, list the hardware and software versions that you require to integrate Siemens and Polycom products using the Siemens OpenScape Video solution. The hardware and software listed in these tables has been verified in a lab environment for use with the Siemens OpenScape Video (V6) solution. Neither Siemens nor Polycom can verify that the solution will work using hardware or software versions other than those listed here.

Table 1-1: Verified Polycom Product Versions

Polycom Product	*Release*
Polycom® Converged Management Application™ (CMA™) 5000/4000	6.0.1
Polycom® Distributed Media Application™ (DMA™) 7000	5.0
Polycom® HDX® Series	3.0.5
Polycom® RMX® 1500 | 2000 | 4000	7.7
Polycom® VVX® 1500 Business Media Phone	4.0.2
Polycom® RealPresence® RPX™, OTX™, ATX™ Immersive Theater Solutions	3.0.5

Table 1-2: Verified Siemens Product Versions

Siemens Product	*Release*
Siemens OpenScape Personal Edition	V6
Siemens OpenScape UC Enterprise Web Embedded Client	V6
Siemens OpenScape UC Application	V6
Siemens OpenScape Voice	V6
Siemens OpenStage Desktop Phones	V3

Finding Help and Support Resources

- For more information about installing, configuring, and administering Siemens OpenScape products, refer to Siemens Support.
- For more information about installing, configuring, and administering Polycom video products, refer to Polycom Video Support.
- For more information on Polycom Converged Management Application (CMA), refer to Polycom CMA Video Resource Management.
- For more information about Acme Packet products, refer to Acme Packet Technical Support.

Chapter 2: Understanding the OpenScape Video Solution Features

This chapter provides an overview of the features offered with Siemens OpenScape® Video solution. OpenScape Video enables you to make video calls by dialing a phone number, and to start or stop video with the press of a single button. You can integrate mixed media collaboration sessions and your existing client applications with OpenScape Video and Voice, for example, by incorporating your voice contact list and presence status into your video solution. You can use video endpoints to communicate with others using video or audio devices such as Open Stage desktop phones, mobile handsets, and smartphones including iPhones or Android-based phones.

When combined with OpenScape Video solution, the En*tera*sys® Secure Networks™ can deliver location services for Polycom telepresence end systems, including detection, authentication, and authorization of telepresence end point systems that are independent of the network vendor.

Understanding OpenScape Unified Communications

This section provides details on OpenScape UC services, devices, features, and desktop application clients.

OpenScape UC Services

OpenScape UC for enterprises typically includes the following services:

- OpenScape Voice, which enables voice or video connections based on an E.164 number that you dial.
- A scalable RMX system that enables integration of several video sources to a single DMA.
- An application server that enables conference participants to share data or collaborate on a single document.

OpenScape UC Devices

OpenScape UC for enterprises supports a number of communication devices, including:

- **Audio Devices** Desktop phones, mobile phones, loudspeakers, and room sound systems
- **Video Devices** PC monitors, webcams, mobile cameras, LCD screens, and HD room cameras
- **Electronic Documents** Word processors, spreadsheets, slide presentations, virtual white boards

OpenScape UC Features

OpenScape UC supports the following features:

- View the status of your contacts while in a video call when using Siemens OpenScape UC Enterprise Web Embedded Client
- Select your preferred video endpoints for incoming and outgoing calls
- Manage your presence information and assign your presence status to video endpoints
- Add entries to your personal address book or to a buddy list
- Collaborate with others using any number of video devices, including OpenScape desktop phones, mobile devices, and smart phones
- Use OpenScape UC desktop application clients, including the Siemens OpenScape Personal Edition and the OpenScape UC Enterprise Web embedded Client, to enable
  - Full HD-capable desktop video
  - Voice to video media escalation

The following diagram illustrates some of the ways you can collaborate using OpenScape UC environments:

Figure 2-1: Example OpenScape UC Environment

Integrating OpenScape Video and OpenScape Voice

OpenScape Video with OpenScape Voice V6 and OpenScape UC Applications support the following features.

- Video calls to and from:
  - Siemens OpenScape Personal Edition V6 client
  - Polycom® VVX® 1500 Business Media Phone running Polycom® UC Software version 4.0.2

  - Polycom® HDX® Series version 3.0.5
  - Polycom® RMX® 1500/2000/4000 version 7.7
  - MCUs managed by Polycom® Distributed Media Application™ DMA™ 7000 version 5.0
  - Polycom® RealPresence® RPX™, OTX™, ATX™ Immersive Theater Solutions version 3.0.5
- Calls between video clients and endpoints by dialing an E.164 number
- Contact lists and global address books foe use with video calls

Understanding Mixed-Media Collaboration Sessions

You can use OpenScape UC to establish connections between different types of endpoints and client applications. For example, you can hold a conference among participants using mixed-media audio or video clients, video conferencing systems, desktop video conferencing systems, and audio-only systems such as telephones and mobile phones. The flexibility of OpenScape UC enables you to share presentations, graphics, and spreadsheets, and to manage collaborative meetings among local, remote, and mobile participants using all kinds of client applications or devices.

In cases where a room system does not support web collaboration, you can connect a computer with collaboration applications to the room system. For example, you can use the Polycom HDX 7000 system to send video and computer information as a combined video stream to the MCU.

A mixed-media conference collaboration can include the following hardware and software components:

- A Polycom HDX 7000 room system
- A Polycom RMX 2000
- An OpenScape Desktop client and OpenScape Web Collaboration on a computer
- A Polycom HDX series system with a computer for OpenScape Web Collaboration

You can establish a video call by dialing the number of the MCU using the E.164 format as you do a traditional audio conference. The OpenScape voice server handles call control for the audio and video calls. Once the video streams are mixed in the Polycom RMX series, you can use the video-enabled UC application clients to participate in telepresence meetings. You can control collaboration using a centralized application server through a web application such as OpenScape Web collaboration using HTTP or HTTPS.

Using Interdomain Video

OpenScape Video connects workers from outside the enterprise domain to workers inside the enterprise domain. Interdomain video requires you to assign outside workers to the organization’s OpenScape Video system. OpenScape Video offers two methods for setting up interdomain video. You can set up a session border controller (SBC) in gateway mode, or you can use a virtual private network (VPN). Each of these methods is explained next.

SBC-Based Interdomain Video

SBC-based video uses Acme Packet Net-Net 3820 to enable voice and video SIP calls between OpenScape endpoints and SIP endpoints in a public or private domain. See Table 1-2: Verified Siemens Product Versions for a list of endpoints that can be connected using an SBC. See SBC at Acme Packet for more information.

VPN-Based Interdomain Video

You can connect OpenScape Video endpoints to SIP endpoints in a public or private domain using VPN.

Using En*tera*sys with OpenScape Video

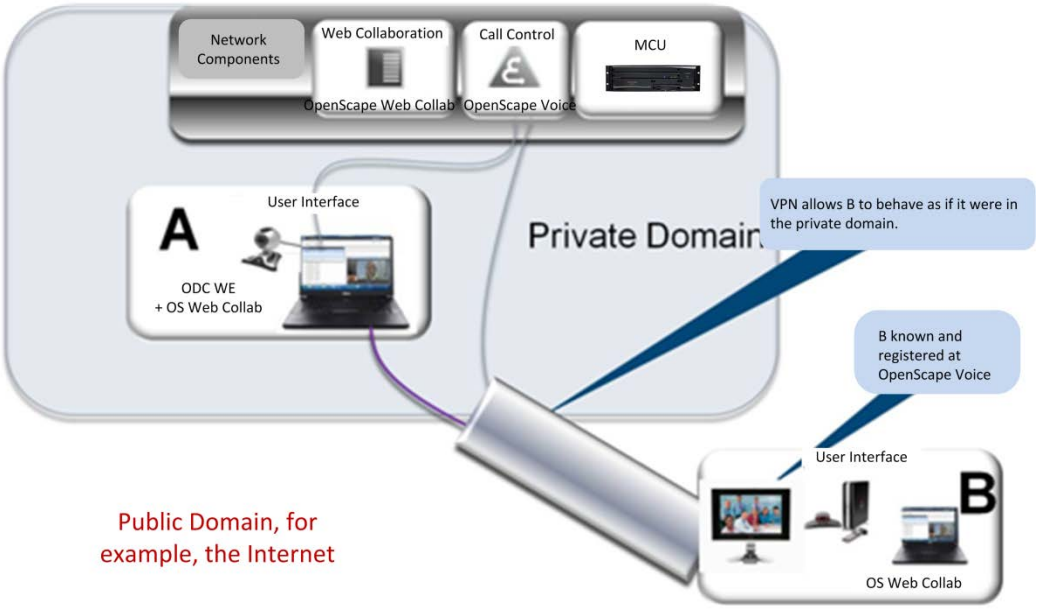
En*tera*sys enables location services for Polycom video endpoints, providing a way to authenticate and authorize video room and desktop systems independently of the network vendor. Enterasys also reduces operation costs by automating asset information updates, detecting unauthorized end systems, and by automating the add, move, and change process. By automatically assigning Quality of Service (QoS) and security profiles, you can improve the reliability and security of video calls and conferences.

Chapter 3: Understanding the OpenScape Video Architecture

This chapter provides an overview of the Siemens OpenScape® Video architecture.

The OpenScape video architecture includes several layers, each of which is explained in this section. The following figure provides an overview of the architecture of the OpenScape Video solution.

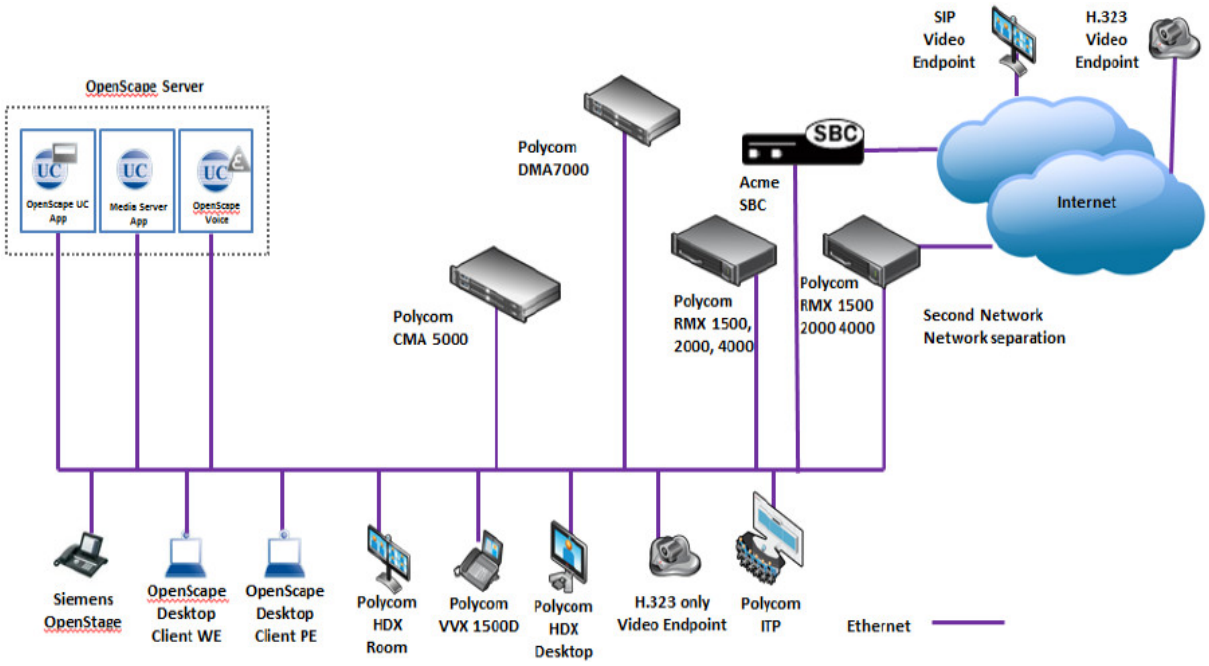
Figure 3-1: Overview of OpenScape Video Solution



Physical Layer

The following diagram illustrates the main connections of the physical layer of the OpenScape Video solution. All physical devices and connections must be on the same network and you must connect external devices to the network using the SBC.

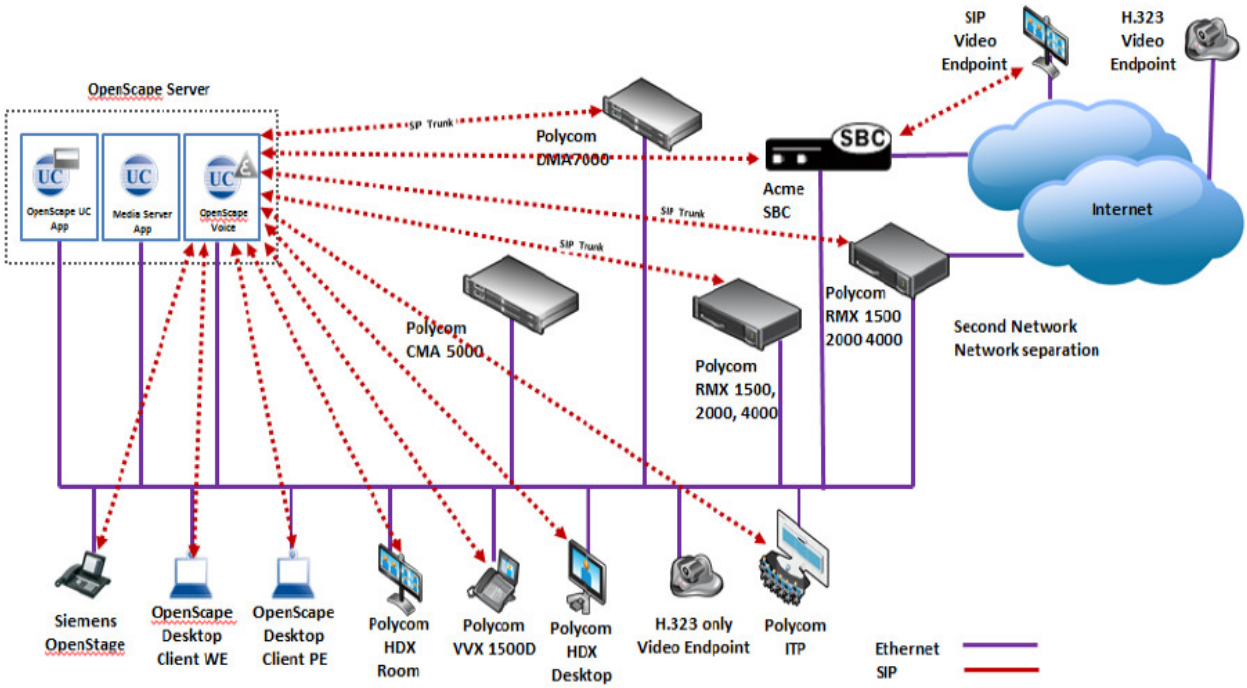
Figure 3-2: The Physical Layer



Session Initiation Protocol (SIP) Layer

The OpenScape Video solution components connected via SIP are shown in the following figure.

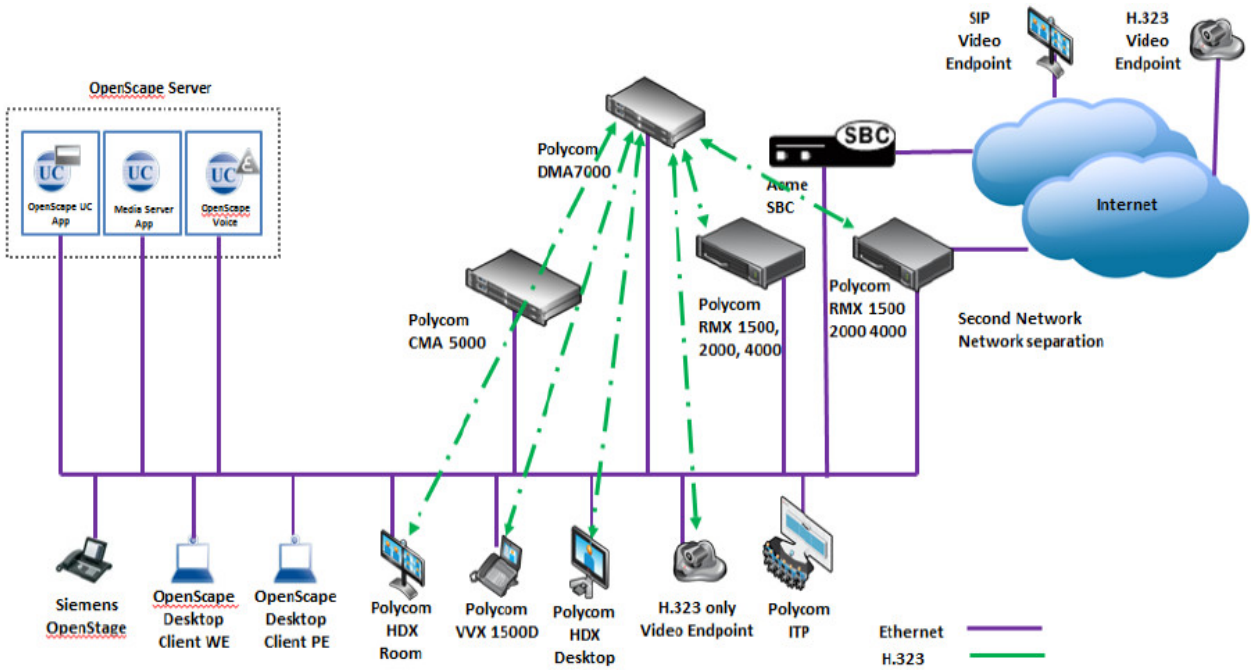
Figure 3-3: The SIP Layer



H.323 DMA System as Gatekeeper

The following illustration shows how non-SIP and H.323 DMA system components register with the OpenScape Video solution. Non-SIP solutions are explained in more detail in the following section Using Non-SIP Components.

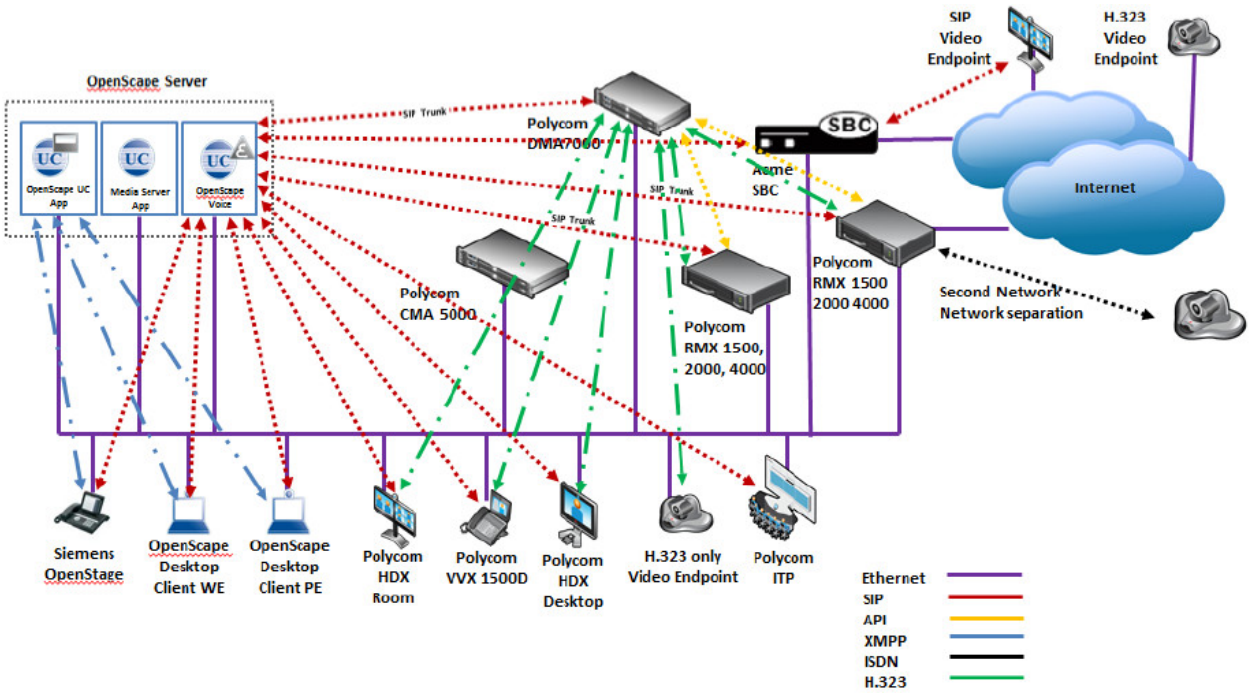
Figure 3-4: H.323 DMA System as Gatekeeper



Overview of the OpenScape Video Solution

The following diagram illustrates the physical, SIP, and H.323 DMA system layers combined.

Figure 3-5: Overview of Video Architecture



Using Non-SIP Components

You can connect to OpenScape video solution using non-SIP components and signaling, including H.323 signaling, proprietary signaling, legacy ISDN non-IP systems, and dual video solutions that use H.323 and SIP. You can adapt, extend, or overlay the OpenScape video solution with your existing non-SIP video deployments.

Connecting H.323 Video Endpoints OpenScape Video

You can use SIP signaling to connect H.323 video endpoints to the OpenScape Video solution in the following example scenarios:

- You can use a Polycom RMX system to connect H.323 video to SIP video endpoints registered to OpenScape Video.
- You can use the Polycom DMA system to support an H.323/SIP Gateway.
- You can support H.323 endpoints by using the RMX as a bridge.
- You can support H.323 endpoints by using the DMA system as the gateway.

Connecting non-IP Video Endpoints to OpenScape Video

You can connect legacy video endpoints such as H.320 and even some proprietary protocols to the OpenScape video solution using an H.320 to H.323 or SIP gateway. You can make these connections using a Polycom RMX, which offers an H.320 to SIP or H.323 interface and supports an H.323/SIP Gateway.

Chapter 4: Understanding OpenScape Video Use Cases

This chapter illustrates several typical use cases you can set up for interdomain video, location and identity assurance (LIA), and virtual multipoint control units (MCUs).

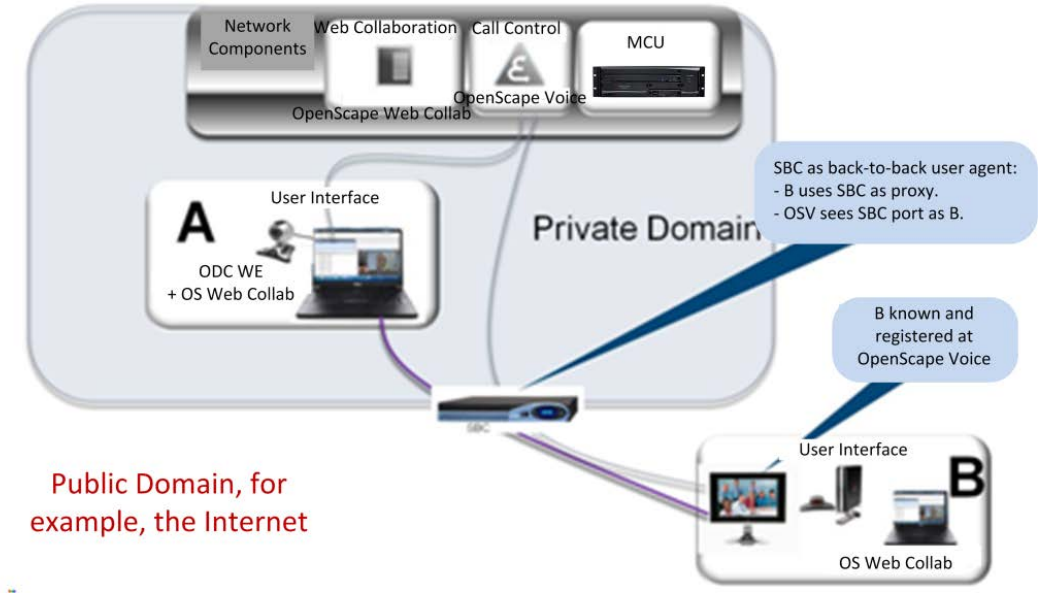
Understanding Interdomain Video Solutions

The Siemens OpenScape® Video solution provides SBC-based interdomain video, VPN-based interdomain video, and gateway-based interdomain video. Each of these solutions is explained next.

Session Border Controller (SBC)-Based Interdomain Video

In a typical SBC use case, an organization with a video room system wants to connect one or more participants in separate locations to their private domain. For example, an organization is holding a conference and wants to add a conference participant located outside of the organization's private domain. In this example, both parties are registered through OpenScape Voice. An SBC handles the network address translation (NAT) and connects the two parties, as shown in the following figure.

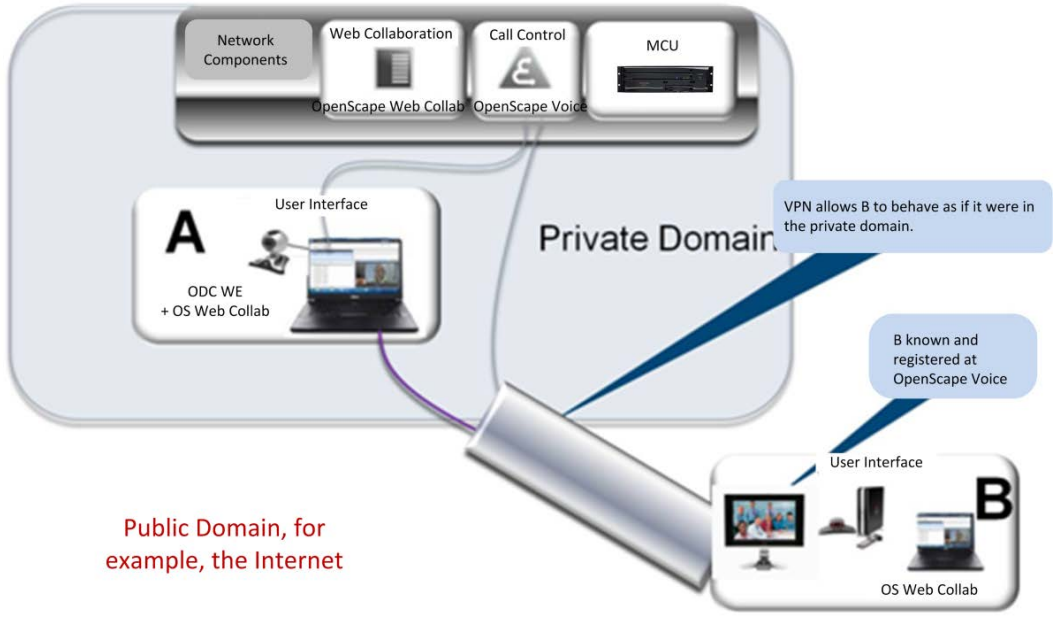
Figure 4-1 : Connecting with an SBC



VPN-Based Interdomain Video

Remote or mobile workers in the public domain can use a virtual private network (VPN) to connect to a private domain and participate in a conference. The benefit of using a VPN to connect is that you can use public services and applications just as you do in the in the private domain. The following figure shows a VPN-based interdomain video solution.

Figure 4-2: Connecting with VPN



Gateway-Based Interdomain Video

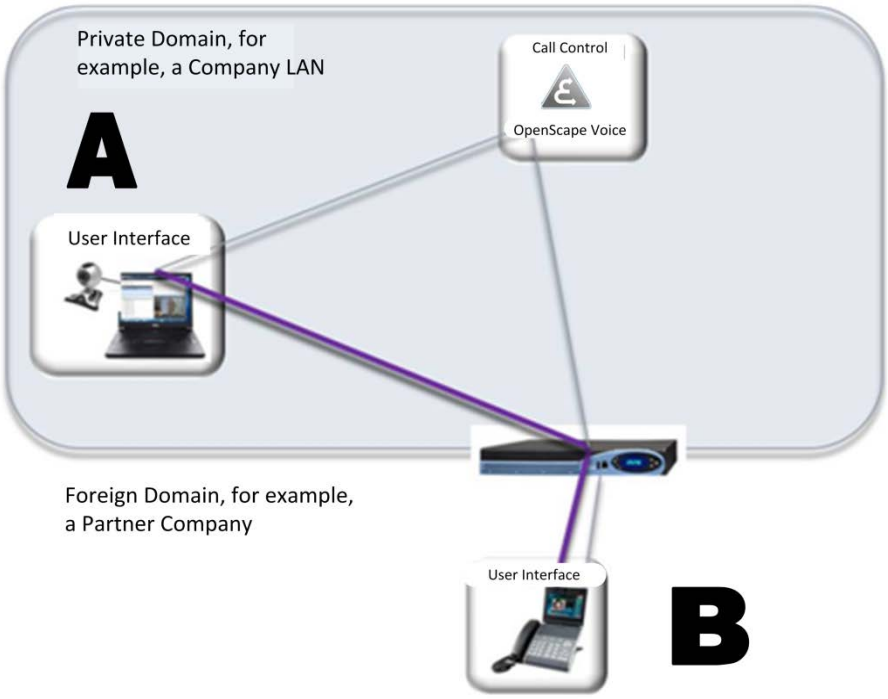
Gateway-based video enables you to connect video-capable endpoints across networks, when endpoints are registered with different SIP registrars. You can use gateway-based interdomain video in the following scenarios:

- To establish a video conference between two endpoints registered with different SIP registrars, for example, a video partner call between an OpenScape product and a Polycom employee.
- To establish a video conference between multiple endpoints registered at different SIP registrars and an on-site MCU. For example, you want to establish a video conference call between an OpenScape product and Polycom product. The conference call is hosted on a Siemens Enterprise Communications product.
- To establish video between video endpoints registered at different SIP registrars and an off-site MCU. For example, you want to establish a video conference call between an OpenScape product and a Polycom product. The conference call is hosted on a Polycom bridge.

- To establish a video conference between multiple parties each registered with a different SIP registrar. For example, Siemens Enterprise Communications employees are registered to OpenScape Voice with Siemens Enterprise Communications and Polycom employees are registered to an OpenScape Video hosted by Polycom.

The following figure illustrates how endpoints registered with different SIP registrars can establish a video conference.

Figure 4-3: Endpoints Registered with different SIP Registrars



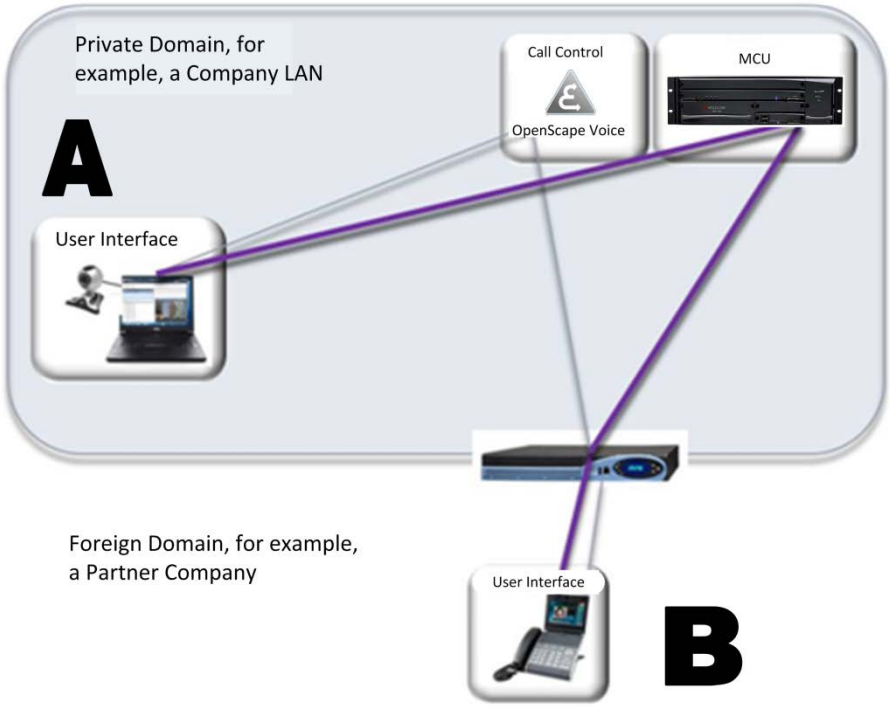
This figure illustrates a typical gateway video call. The video conference can be initiated at endpoint A in a private domain, for example, `siemens-enterprise.com`, or at endpoint B in a partner company domain, for example, `polycom.com`.

The incoming call from B to A in the private domain is established by dialing in the format `domain_name@privatedomain.com`, for example, `27111@siemens-enterprise.com`. The outgoing call from A to B is established by dialing the gateway number, for example, 99 plus the domain name of the called partner, `99 13131`. After receiving the number, the gateway deletes 99 from the string and adds `@polycom.com`. The called party is addressed by `13131@polycom.com`.

Connecting Multiple On-Site Video Endpoints

You can connect multiple video endpoints within the same network for a video conference. The following figure shows an example of multiple video endpoints registered at different SIP registrars with an on-campus MCU.

Figure 4-4: Connecting Multiple On-Site Video Endpoints



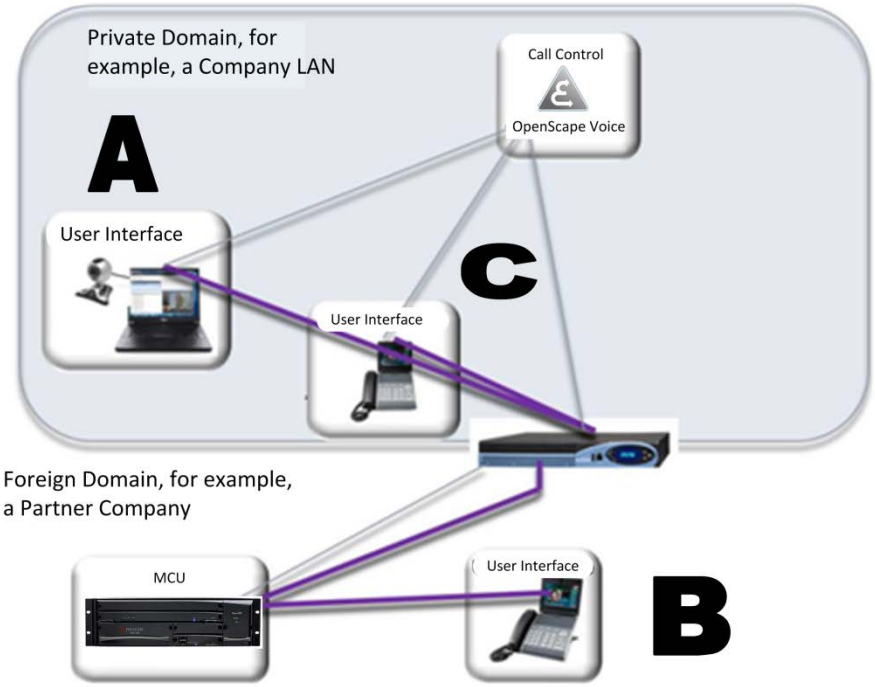
This figure illustrates an example of a video conference established between two registered partners using an MCU in the private domain of one of the partners. For example, a representative of Siemens Enterprise Communications wants to meet with a Polycom associate using a Siemens MCU address `siemens-enterprise.com`.

User A calls into the MCU with the domain name, for example, `88888`. User B dials into the MCU by dialing `domain_name@private domain.com`, for example, `88888@siemens-enterprise.com`.

Connecting Multiple Off-Site Video Endpoints

You can use an off-site MCU to establish video conferences between multiple off-site video endpoints, each registered with a different SIP registrar. The following diagram illustrates how multiple partners, such as Siemens Enterprise Communications and Polycom, can connect for a video conference using an MCU in the private domain, for example, as `siemens-enterprise.com`.

Figure 4-5: Connecting Multiple Off-Site Video Endpoints



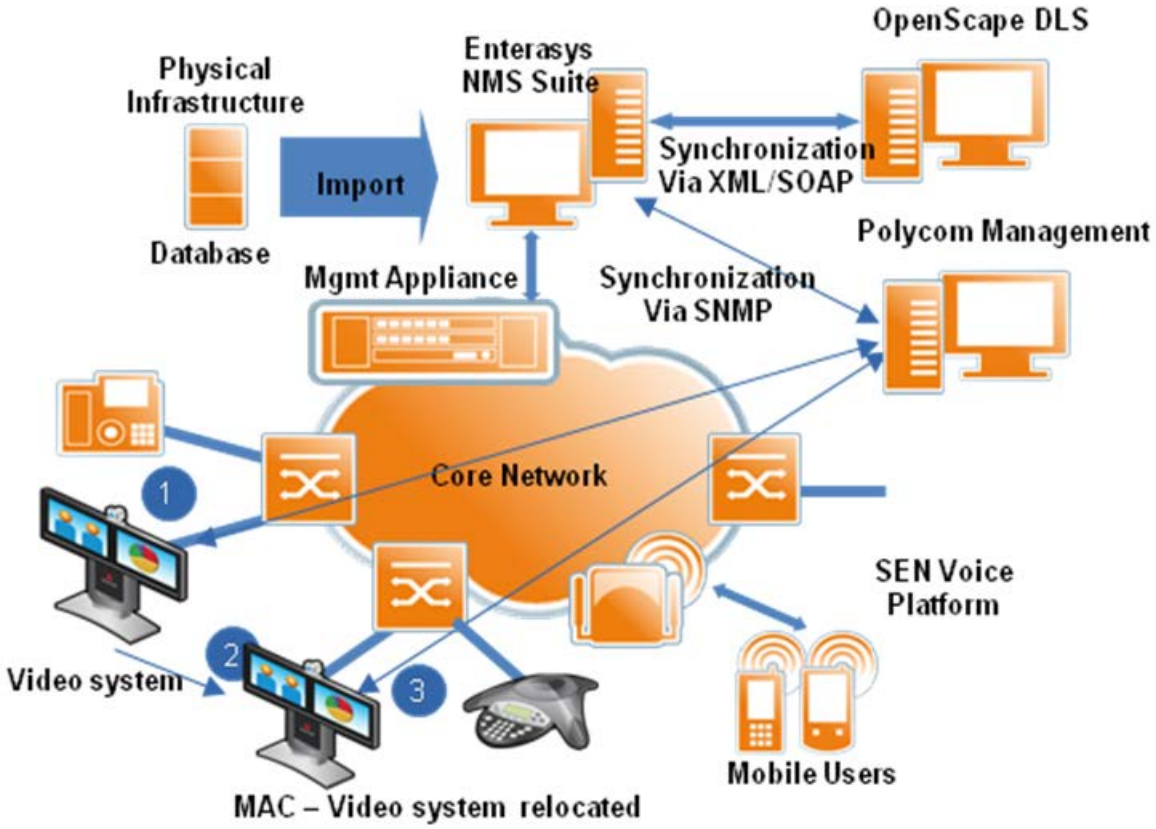
Users A and C call into the MCU in the Siemens network by dialing the gateway number, for example 99 plus the domain name of the partner, `99 77777`. After receiving the number the gateway deletes 99 from the string, adds `@siemens-enterprise.com`, and addresses the MCU with `77777@ siemens-enterprise.com`. User B can dial `domain_name@partner` domain, that is, `77777@ siemens-enterprise.com`, or dial `77777`.

Understanding OpenScape Location and Identity Assurance (LIA) Network Automation Support for Polycom Video Endpoints

The OpenScape location and identity assurance (LIA) solution provides a location service database for all kinds of end-user systems, including new, moved, or reconfigured users. This feature helps to reduce operational costs while increasing the productivity of administrators and users. Higher availability and reliability guarantees continuity of business processes for enterprises.

OpenScape LIA also improves the security of video calls and conferences by automatically assigning Quality of Service (QoS) and security profiles called Policies using a network access control (NAC) solution.

The following figure shows several Polycom endpoints supporting a location and identity assurance (LIA) network automation, and is followed by more detail on QoS.



Understanding Quality of Service

Quality of Service (QoS) is an important prerequisite for voice and video over internet protocol (IP). OpenScape LIA enables you to automatically assign and track QoS profiles for all OpenScape Video devices and clients as well as the Polycom HDX series system and VVX 1500 phones. The challenge is to guarantee that packet traffic and media connections are not delayed or dropped as a result of interference from IP traffic. Typical QoS problems include:

- **Latency** Delays in packet delivery
- **Jitter** Variations in delay of packet delivery
- **Packet loss** Heavy network traffic causing dropped packets

You must ensure that your HDX series system or VVX 1500 phone is registered to or monitored by the CMA system. The Enterasys Network Management System (NMS) pulls the endpoint information from the CMA system via Simple Network Management Protocol (SNMP) in the following order:

1. The Enterasys Network Management System (NMS) imports data from the physical infrastructure, such as switches and routers, and from the database.
2. The Enterasys Network Management System (NMS) communicates with the management appliance to identify the switch the port that is connecting the HDX system or VVX 1500 phone.
3. The management appliance applies the QoS and security settings (also known as policies) for these ports based on the policy it has received from the Enterasys Network Management System (NMS).

Using Virtual MCUs in OpenScape Video

Polycom® Distributed Media Application™ (DMA™) 7000 system enables you to configure virtual MCUs, including multiple physical MCUs that you can access as a single MCU. The benefit of this solution is better scalability, load balance, and network simplification. The DMA system identifies failure of a physical MCU or data path and automatically switches to an alternate MCU. As a result, video conferences are interrupted only briefly.

Connecting Redundant MCUs Using the Polycom DMA System

The Polycom DMA system, shown in the following illustration, enables you to control several MCUs as one virtual MCU by balancing the load to each connected MCU. This prevents loss of service if a bridge goes down, and reduces the capacity of only the virtual MCU.

Figure 4-6: The Polycom DMA System

The DMA system supports resilient video conferencing, conference call failover if a connection to a bridge fails during a call. The DMA system automatically holds the call and reestablishes the connection to another bridge. Video conference participants notice little break in video and might see a short period of still video while the system is reconnecting.

Because you can control several MCUs with the DMA system, you can migrate deployment scenarios from the Polycom RMX system to another manufacturer's MCU or vice versa.

Refer to the following section for more information on use cases that the DMA system supports.

Use Cases for Resilient Video Conferencing

The following section explains use cases for resilient video conferencing.

Centralized Conference Resource Management

You require a centralized conference resource management application to create a pool of conference servers that behave as one large conference server. This management application server tracks the incoming calls and routes them to the appropriate resource, for instance, based on available server resources or on available bandwidth to the location of this server.

If the virtual meeting room (VMR) is using a template that has cascading enabled, the application server automatically creates cascading links. The DMA system must have site topology data. For more information, refer to the Polycom DMA system documentation at support.polycom.com.

Cascading a video conference across multiple MCUs can conserve bandwidth and is especially useful when using wide area network (WAN) links. Specifically, participants can connect to MCUs that are geographically near, reducing network traffic between sites to a single link to each MCU. Cascading does, however, impact the quality of the conference experience.

Note: Cascading is Supported for RMX MCUs in H.323

Cascading is supported only for RMX MCUs and only in H.323. The Polycom DMA system must be configured to support H.323 signaling in order to enable cascading. For conferences with cascading enabled, the system selects only RMX MCUs that have H.323 signaling enabled.

The management application provides uninterrupted service by routing calls around failed or busy media servers. It also allows media servers to have a busyout status during maintenance activities. From the user's point of view, the service is always available. The system can gradually grow from small deployments of one-to-two media servers to large deployments with many geographically dispersed media servers. System administrators can monitor daily usage and plan the expansion as necessary.

This approach also provides a centralized mechanism to deploy a front-end application to control and monitor conferencing activities across all media servers. The management application acts as a load balancer in this scenario, that is, it can distribute the load over a group of conference servers. The larger the resource pool, the more efficient the load balancing function, a feature that is critical to large organizations with offices and conference servers around the world.

The same technology can be used by service providers who offer conference services globally by using the Polycom DMA 7000 solution and deploying conference servers in central points of the network. The scenario works well in architectures such as SIP, in which the registrar function is separate from the proxy function, that is, where the endpoint is registered with a SIP registrar in the network but sends its calls to a pool of SIP Proxies.

Automatically Routing Around Outages

The Polycom DMA system receives notification if a bridge goes down or becomes full, and responds to prevent loss of service. Only the capacity is reduced during the outage.

In the case of a conference call failover, that is, if a connection to a bridge fails during a call, the DMA system automatically holds the call and reestablishes it on another bridge. End users and administrators do not have to intervene.

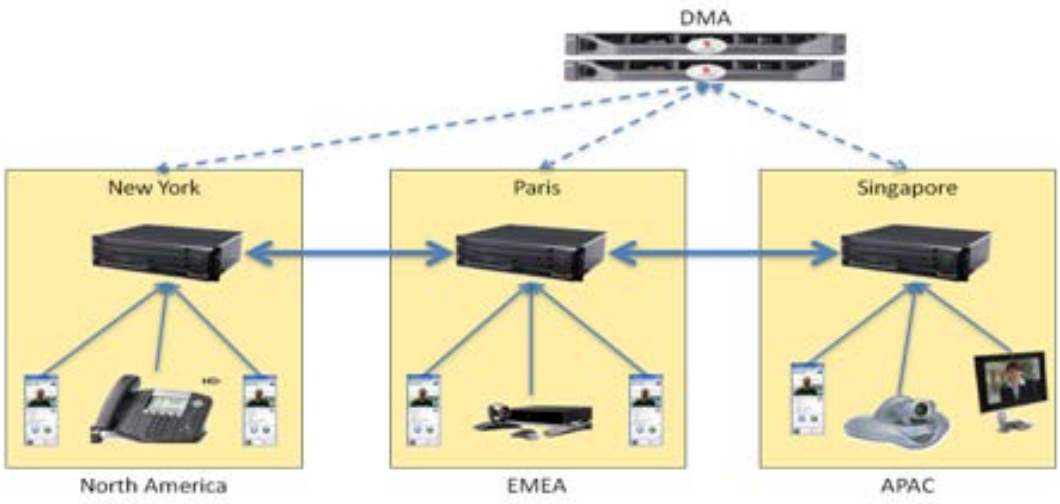
The following table lists features of the Polycom DMA system.

Figure 4-7: Features of the Polycom DMA System

Feature	*Description*
Scalability - Smart Capacity Growth	• Addition of another DMA server for redundancy • Add more MCUs • Provisioning of VMRs the same as for Medium deployment
Supported MCU Capacities	• DMA system supports up to 64 bridges • Supports 1,200 concurrent calls: Video, audio, CIF, HD • Tested to 375,000 Active Directory users • Supports Polycom RMX 1500/2000/4000 bridges • Also applicable for Cisco Codian
MCU Auto Cascading	• All users dial same VMR number, regardless of location • DMA system routes calls to the closest bridge • DMA system establishes links between bridges • Users do not have to modify their dialing behaviors

The following figure illustrates use of the DMA system as a centralized conference resource management application.

Figure 4-8: Using the DMA System as a Centralized Conference Resource Management Application



Chapter 5: Configuring Siemens OpenScape Voice

This chapter shows you how to configure Siemens OpenScape® Voice.

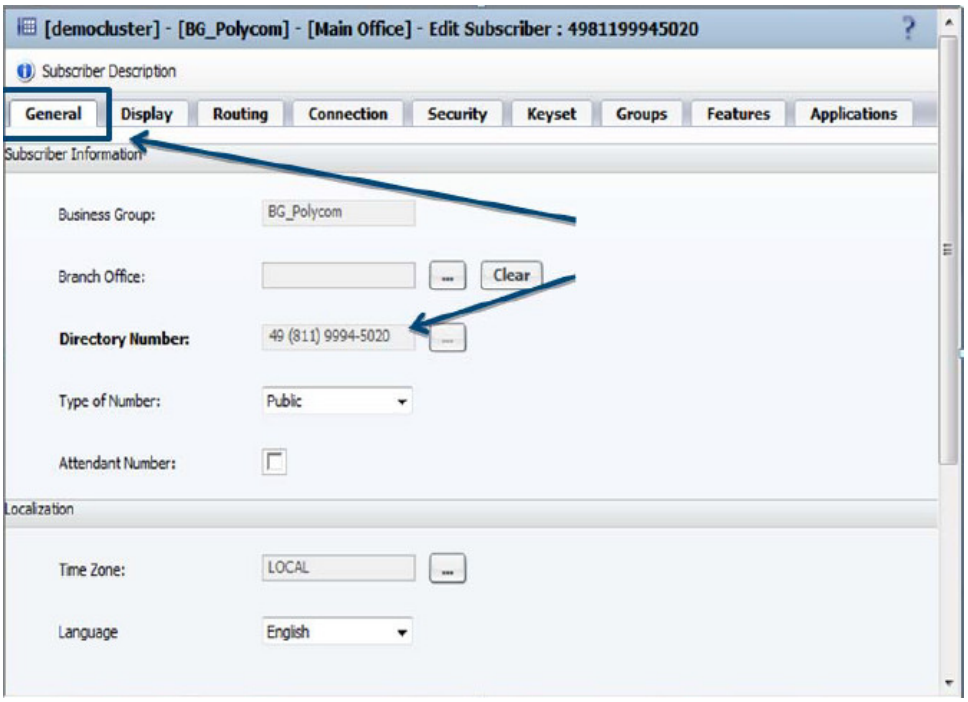
Configuring OpenScape Voice Subscriber

This section shows you how to configure OpenScape voice subscriber properties.

To configure OpenScape Voice Subscriber properties:

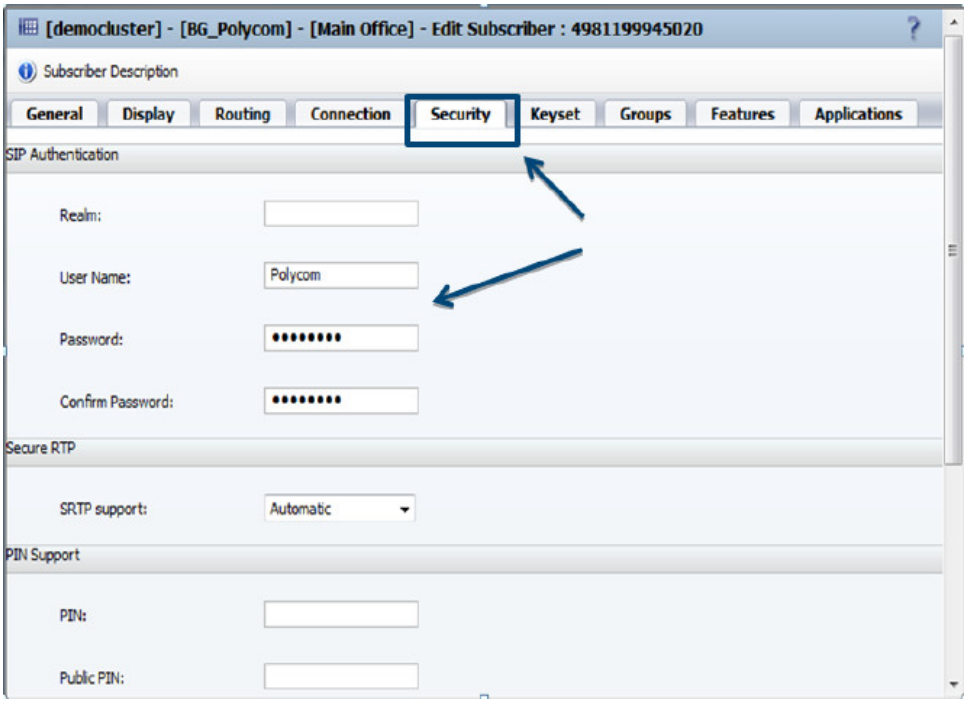
1. Open the Common Management Portal.
2. Go to **OpenScape Voice** > **Business Group** > **Members** > **Subscribers.**
3. Click on the directory number you want to modify or check.

   The Edit Subscriber dialog displays:



4 In the Edit Subscriber dialog, choose the **General** tab and enter a number in the **Directory Number** field**.** The number you enter here is used in the SIP configuration of the HDX system as the **User Name** field. You can access this number for the HDX in the User Name field of the HDX SIP settings, as shown in Specifying HDX SIP Settings. You can access this number for the VVX 1500 phone in the SIP settings of a registered line. These SIP settings are available in the Web Configuration Utility, as shown in Configuring Polycom VVX 1500 and SIP Settings.

5 In the Subscriber dialog, choose the **Security** tab and enter the user name and password in the **User Name** and **Password** fields, as shown next.



These two fields configure HTTP Digest Authentication. You can access the user name and password for the HDX system in the Domain User Name and Password fields of the HDX SIP settings, as shown in Specifying HDX SIP Settings. You can access this number for the VVX 1500 in the Authentication User ID and Authentication Password fields in the Web Configuration Utility.

Configuring OpenScape Voice Endpoints

This section shows you how to configure OpenScape voice endpoints.

To configure OpenScape Voice Endpoint properties:

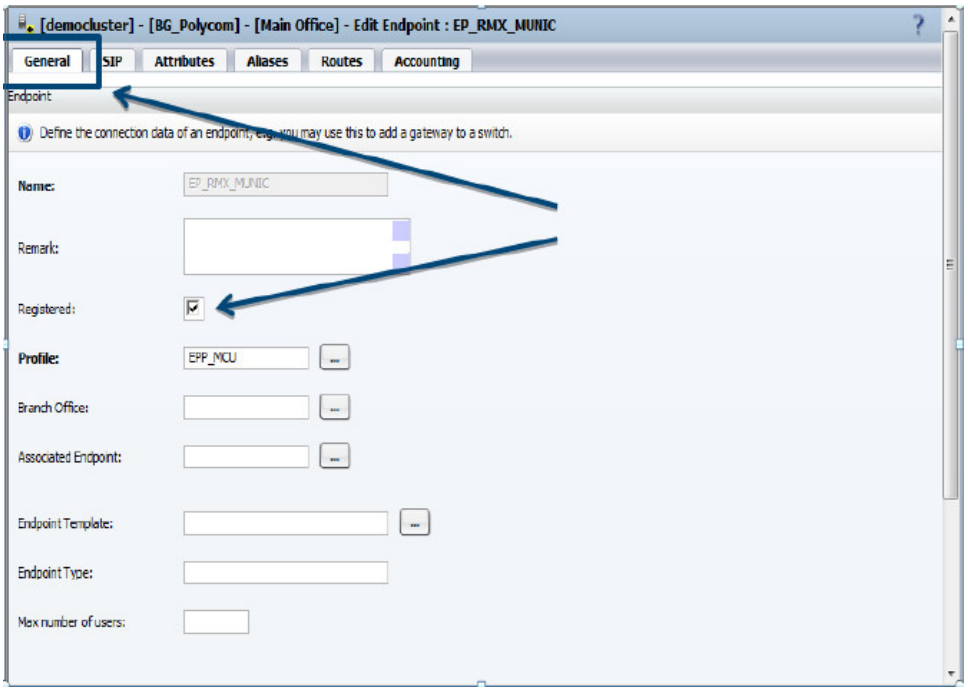
1 Open the Common Management Portal.

2 Go to **OpenScape Voice** > **Business Group** > **Members** > **Endpoints**.

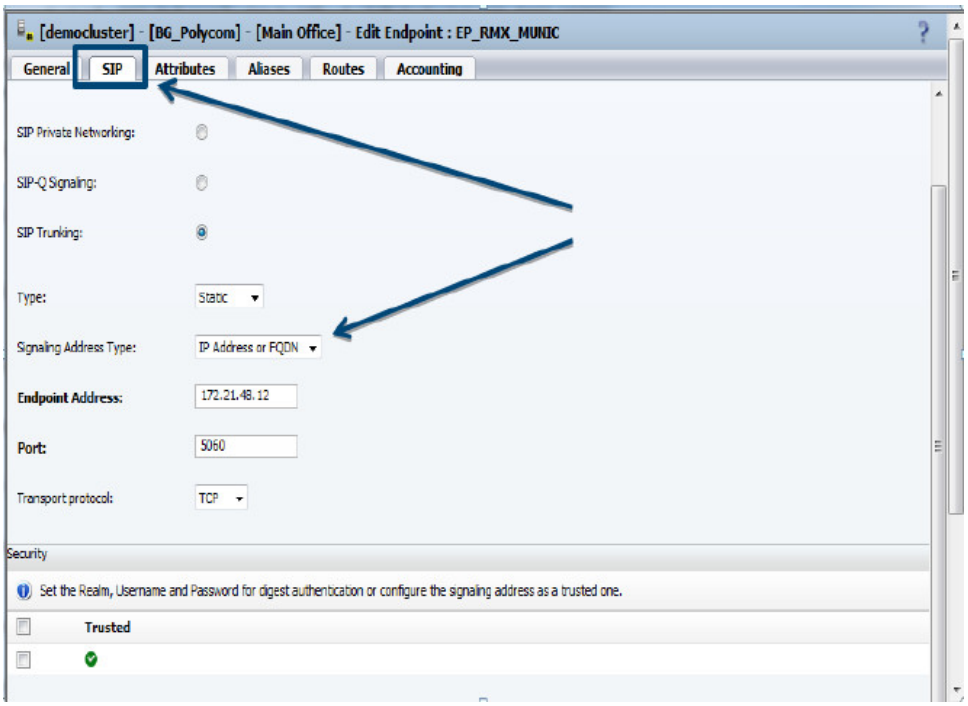
3 Click on the name of the endpoint you want to modify or check.

The Endpoint dialog displays.

4 In the Endpoint dialog, choose the **General** tab and check **Registered**, as shown next.



5 Choose the **SIP** tab, shown next, and set the following fields:



- **Type** Static
- **Signaling Address Type** IP Address or FQDN
- **Endpoint Address** Signaling IP address or FQDN of the RMX system or the DMA system
- **Port** 5060
- **Transport protocol** TCP
- **Endpoint** Trusted

Chapter 6: Integrating Polycom HDX Systems with Siemens OpenScape

This chapter provides an overview of how to set up and configure a Polycom® HDX® system and integrate it with Siemens OpenScape® Voice. Once you configure the Polycom HDX system and integrate it with Siemens OpenScape software version 3.0.5, you can place and receive calls with Siemens OpenScape Desktop Client PE, Desktop Client WE, and Siemens OpenScape Voice version 6. This chapter includes a section that shows you how to set up Polycom's On Demand Conferencing Solution.

For detailed information about configuring HDX systems, refer to Polycom Video Support or the Administrator's Guide for Polycom HDX Systems.

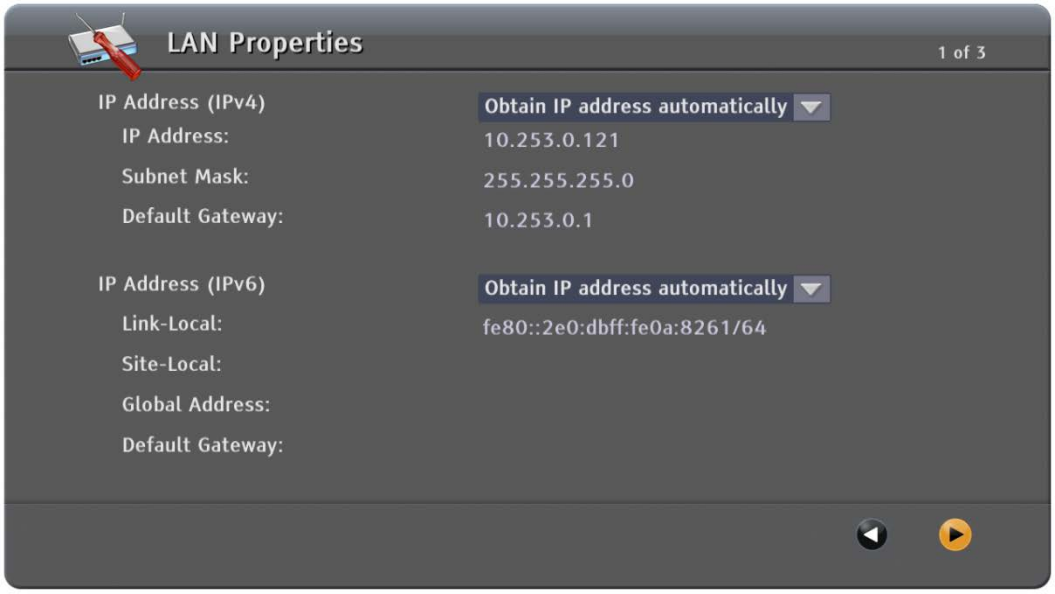
Configuring Polycom HDX Systems LAN Properties

To begin integration, you need to configure HDX system LAN properties. You can configure options for the HDX using the system user interface or the web interface. This procedure shows you how to configure settings using the web interface.

To configure Polycom HDX LAN properties:

1. Do one of the following:
   - In the HDX system user interface, go to **System** > **Administrator Settings** > **LAN Properties**.

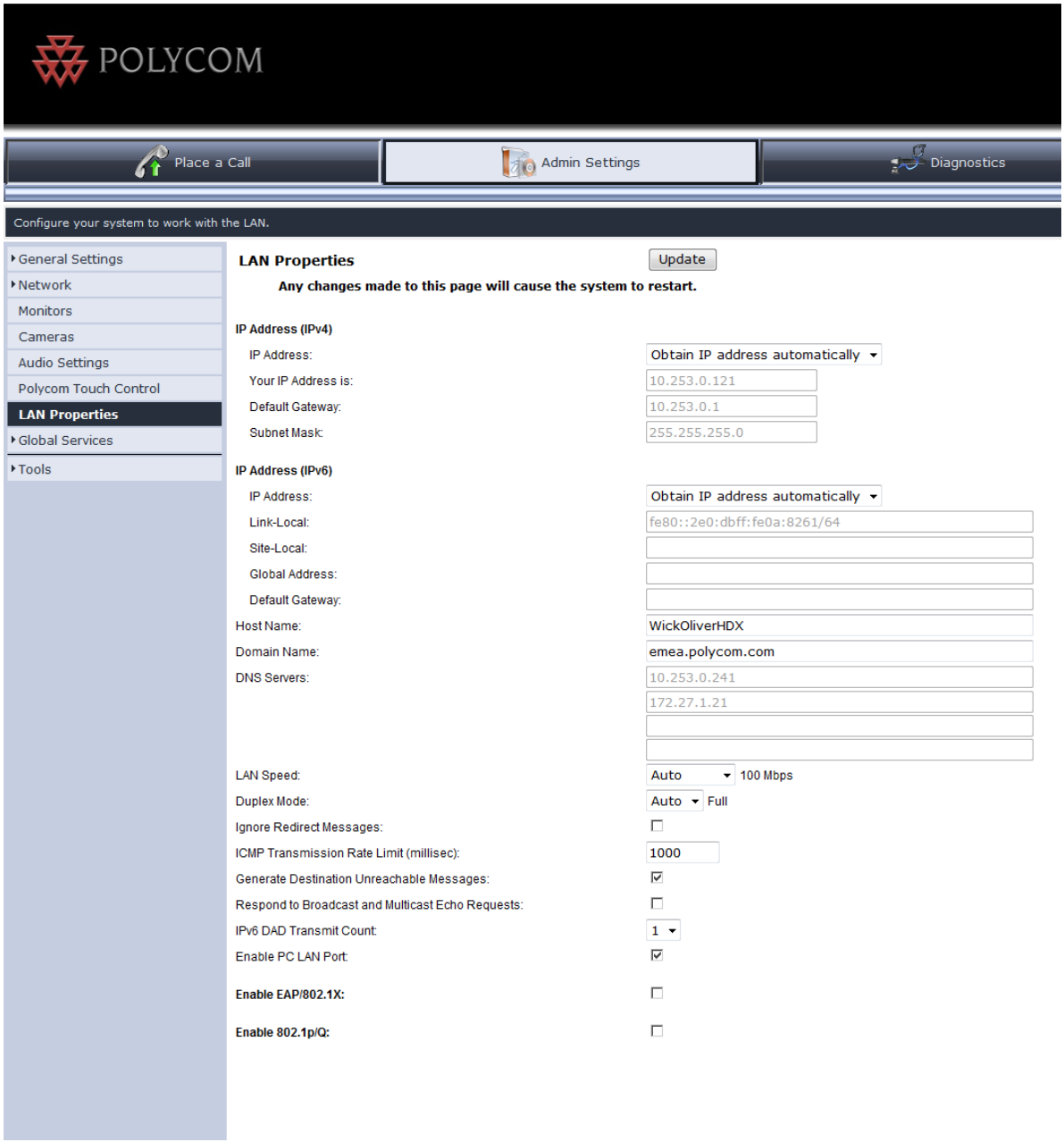
     LAN Properties display, as shown next. Use to navigate multiple pages in the interface.



OR

- In the address bar of your web browser, type in the IP address of your HDX system, press **Enter,** and choose **Administrator Settings** > **LAN Properties**. If your system is password protect, a login dialog displays when you choose Administrator Settings. The default user name is *admin* and the default password is the serial number of your HDX system. If you don't know the password, contact your the system administrator.

  The LAN Properties screen displays, shown next.



Note: Changes to These Settings Require and Cause a System Restart

Changes you make to these settings require a system restart. If you make changes to these settings, the system automatically restarts when you accept the changes.

2 On the LAN Properties screen, configure the following fields:

- **IP Address (Ipv4)**
  - **IP Address**

    Specify how the system obtains an IP address. Choose one of the following options:

    - » **Obtain IP address automatically** Choose this option if the system obtains an IP address from the DHCP server on the LAN.
    - » **Enter IP address manually** Choose this option if the IP address will not be assigned automatically.
  - **Use the Following IP Address**
    - » If you chose to obtain an IP address automatically in the **IP Address** field, the IP address displays currently assigned to the system displays in this field.
    - » If you selected **Enter IP Address Manually**, enter the IP address here.
  - **Default Gateway** This field displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here.
  - **Subnet Mask** This field displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here.

- **IP Address (IPv6)**
  - **IP Address** Specify how the system obtains an IP address. Choose one of the following options:
    - » **Obtain IP address automatically** Choose this option if the system gets an IP address automatically. DHCP is not currently supported for IPv6. When you choose this setting, the system uses Stateless Address Autoconfiguration (SLAAC) to obtain a global address, unique local address (ULA), or site-local address using router advertisements. The network routers also must be configured appropriately to provide the advertisement packets.
    - » **Enter IP address manually** Choose this option if the IP address will not be assigned automatically.
    - » **Off** Choose this option to disable IPv6.
  - **Link-Local** Displays the IPv6 address used for local communication within a subnet.
  - **Site-Local** Displays the IPv6 address used for communication within the site or organization.
  - **Global Address** Displays the IPv6 internet address.

- **Default Gateway** Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here.
- **Host Name** Indicates the system's Domain Name System (DNS) name.
- **Domain Name** Displays the domain name currently assigned to the system. If the system does not automatically obtain a domain name, enter one here.
- **DNS Servers** Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, you can enter up to four DNS servers here.
  - **IPv6** You can specify IPv6 DNS server addresses for IP addresses entered manually or obtained automatically (in the case of a system on a hybrid network that obtains IPv4 DNS server addresses via DHCPv4).
  - **IPv4** You can specify IPv4 DNS server addresses only when the IPv4 address is entered manually. When the IPv4 address is obtained automatically, the DNS Server addresses are also obtained automatically.
- **LAN Speed** Specify the LAN speed to use. Note that the speed you choose must be supported by the switch. You can choose from the following options:
  - Choose **Auto** to have the network switch negotiate the speed automatically. Choosing **Auto** automatically sets **Duplex Mode** to **Auto**.
  - If you choose **10 Mbps**, **100 Mbps**, or **1000 Mbps** you must set **Duplex Mode** to **Half** or **Full**.

Note: LAN Speed Settings for the Polycom HDX and Switch Must be The Same

Polycom does not support **Auto** for the Polycom HDX system only or the switch only; the settings for both must be the same.

- **Duplex Mode** Specify the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch. Choose one of the following options:
  - Choose **Auto** to have the network switch automatically negotiate the Duplex mode. Choosing **Auto** automatically sets the **LAN Speed** field to **Auto**. The duplex settings for both the Polycom HDX system and the switch must be the same. Polycom recommends that you set both to **Auto**.
  - **Half Duplex** Half Duplex provides communication in both directions, but only one direction at a time (not simultaneously).
  - **Full Duplex** Full Duplex allows communication in both directions simultaneously.
- **Ignore Redirect Messages** Enables the HDX system to ignore redirect messages from network routers. A redirect message tells the endpoint to use a different router than the one it is using.

- **ICMP Transmission Rate Limit (millisec)** Specifies the minimum number of milliseconds between transmitted packets. Enter a number between 0 and 60000. The default value of 1000 signifies that the system sends 1 packet per second. If you enter 0, the transmission rate limit is disabled. This setting applies only to *error* ICMP packets. This setting has no effect on *informational* ICMP packets, such as echo requests and replies.
- **Generate Destination Unreachable Messages** Generates a Destination Unreachable message if a packet cannot be delivered to its destination for reasons other than network congestion.
- **Respond to Broadcast and Multicast Echo Requests** Sends an Echo Reply message in response to a broadcast or multicast Echo Request, which is not specifically addressed to the HDX system.
- **IPv6 DAD Transmit Count** Choose to send 1, 2, or 3 Duplicate Address Detection (DAD) messages before acquiring an IPv6 address. The HDX system sends DAD messages to determine if the address it is requesting is already in use.
- **Enable PC LAN Port** Check this box to enable the PC LAN port on the back of Polycom HDX 4000 and 4500, HDX 7000, HDX 8000, or HDX 9006 system. Disable this setting for increased security. This option is not available on the Polycom HDX 6000 or 9000.
- **Enable EAP/802.1X** Check this option to enable the EAP/802.1X authentication protocol. Polycom HDX systems support the following authentication protocols:
  - EAP -MD5
  - EAP-PEAPv0 (MSCHAPv2)
  - EAP-TTLS
  - EAP-TLS
- **Enable 802.1p/Q** Check this box to specify whether VLAN and link layer priorities are enabled. The following optional QoS settings are available only when 802.1p/Q is enabled and only on the web interface:
  - **VLAN ID** Specifies the identification of the Virtual LAN. The value can be any number from 1 to 4094.
  - **Video Priority** Sets the link layer priority of video traffic on the LAN. Video traffic is any RTP traffic consisting of video data and any associated RTCP traffic. The value can be any number from 0 to 7, although 6 and 7 are not recommended.
  - **Audio Priority** Sets the priority of audio traffic on the LAN. Audio traffic is any RTP traffic consisting of audio data and any associated RTCP traffic. The value can be any number from 0 to 7, although 6 and 7 are not recommended.
  - **Control Priority** Sets the priority of control traffic on the LAN. You can choose a value from 0 to 7, although 6 and 7 are not recommended. Control traffic is any traffic consisting of control information associated with a call and can include:
    - **H.323** H.225.0 Call Signaling, H.225.0 RAS, H.245, Far End Camera Control

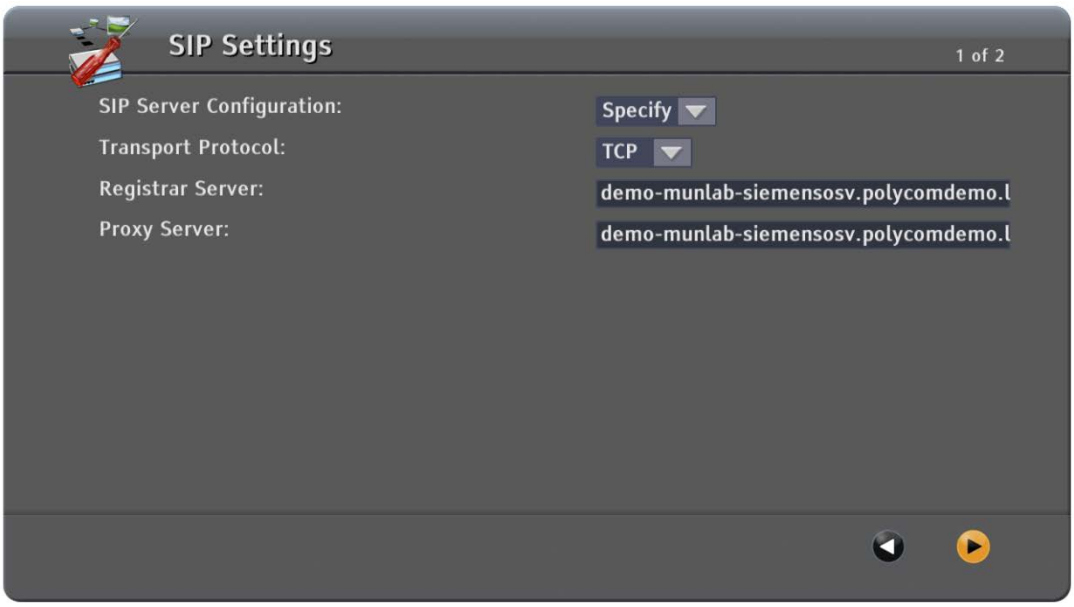
- **SIP** SIP Signaling, Far End Camera Control, Binary Floor Control Protocol (BFCP)

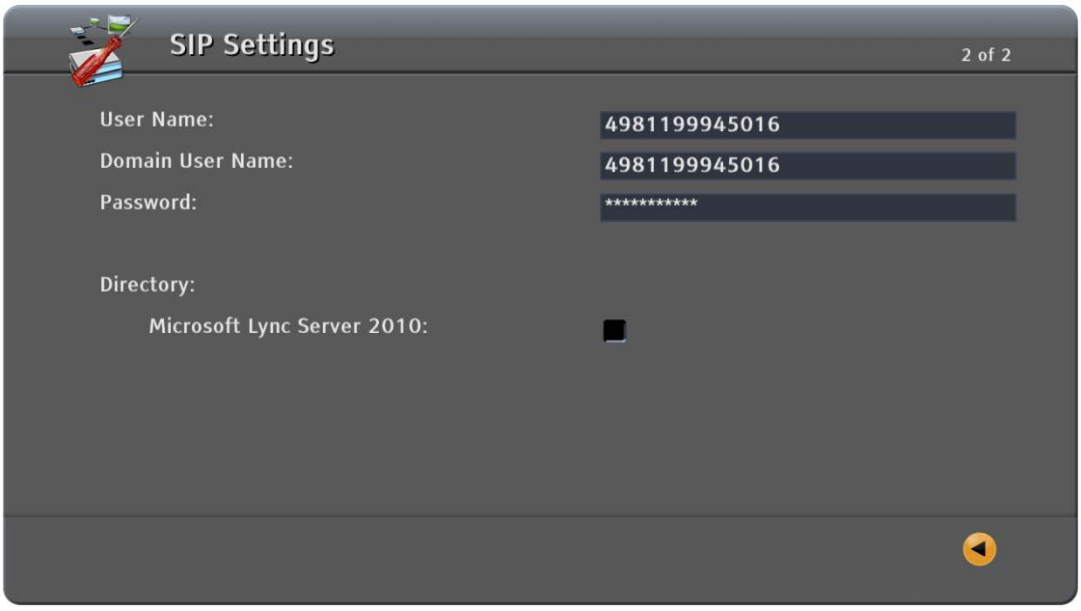
Specifying HDX SIP Settings

Once you have configured the Polycom HDX system LAN properties, specify Session Initiation Protocol (SIP) settings to connect SIP calls using Siemens OpenScape Voice. You can configure SIP settings using the system user interface or the web interface. This procedure shows you how to configure settings using the web interface.

To specify SIP Settings:

1. Do one of the following:
   - In the system local interface, go to **System > Admin Settings > Network > IP > SIP Settings**. The SIP Settings display, shown next. Use to navigate multiple pages in the interface.

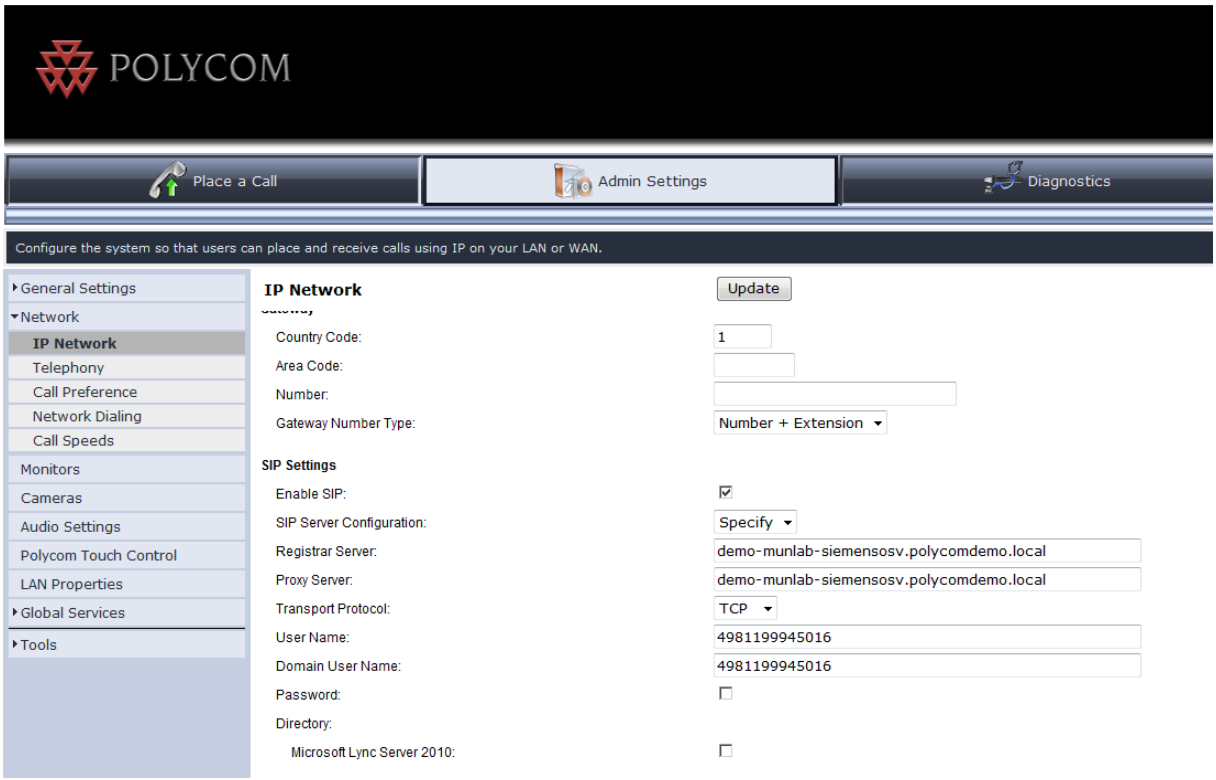




OR

- In the address bar of your web browser, type in the IP address of your HDX system, press Enter, and choose **Administrator Settings > Network > IP Network > SIP Settings**. Note that if your system is password protected, a dialog displays when you choose Administrator Settings.

  The IP Network screen display, shown next.



2 Configure the following settings:

- **Enable SIP** Enable
- **Transport Protocol** This field determines the protocol the system uses for SIP signaling. The SIP network infrastructure in which your Polycom HDX system is operating determines which protocol is required. You can choose from the following options:
  - » **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.
  - » **TCP** provides reliable transport via TCP for SIP signaling.
- **User Name** Enter the directory number of the OpenScape Voice. This field specifies the SIP address or SIP name of the system — for example, `mary.smith@department.company.com`. If you leave this field blank, the system's IP address is used for authentication. In a Siemens environment, this setting is the Subscriber number provided by the OpenScape Voice administrator.
- **Domain User Name** Digest Authentication User Name. This field specifies the name to use for authentication when registering with a SIP Registrar Server — for example, msmith@company.com. If the SIP proxy requires authentication, this field and the password cannot be blank.
- **Password** Digest Authentication Password. This field specifies the password that authenticates the system to the Registrar Server.
- **SIP Registrar Server** OpenScape Voice IP or DNS-Name (preferred). This field specifies the IP address or DNS name of the SIP Registrar Server. By default for TCP, the SIP signaling is sent to port 5060 on the registrar server. By default for TLS, the SIP signaling is sent to port 5061 on the registrar server.

  Enter the IP address and port using the following format:

  <IP_Address>:<Port>

  <IP_Address> can be an IPv4 address or a DNS hostname such as `servername.company.com:6050`. Hostnames can resolve to IPv4 or IPv6 addresses.

  Syntax Examples:

  To use the default port for the protocol you have selected: `10.11.12.13`

  To specify a different TCP or UDP port: `10.11.12.13:5071`

  Enter an IPv6 address using the following format:

  [<IPv6_Address>]:<Port>

  An example of an IPv6 address is: `[2001:db8:85a3::8a2e:370:7334]:8032:8033`

Note: Cascaded multipoint is not supported in SIP calls.

Cascaded multipoint is not supported in SIP calls. For more information about SIP compatibility issues, refer to the *Release Notes for Polycom HDX Systems*.

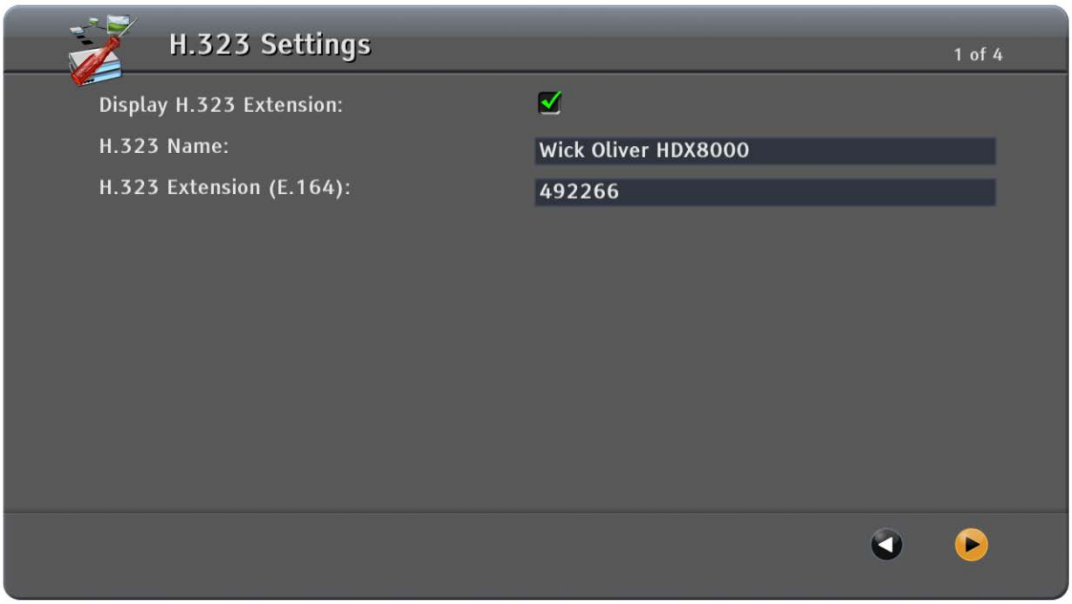
Specifying H.323 Settings (Optional)

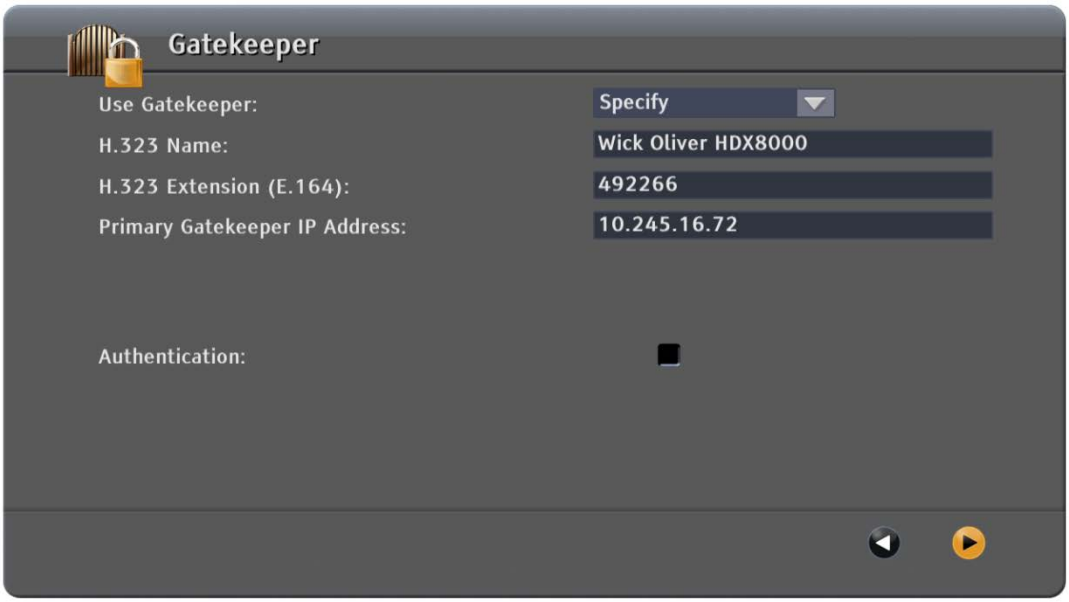
If your network uses a gatekeeper, you can choose to have the HDX system automatically register its H.323 name and extension, enabling others to call the system by entering that H.323 name or extension instead of the IP address. You can configure H.323 settings using the system user interface or the web interface. This procedure shows you how to configure settings using the web interface.

To specify H.323 settings:

1. Do one of the following:
   - In the system interface, go to **System > Administrator Settings > Network > IP > H.323 Settings**.

     The H.323 Settings display. Use to navigate multiple pages.





OR

- In the address bar of your web browser, type in the IP address of your HDX system, press Enter, and choose **Administrator Settings > Network > IP Network**. Note that if your system is password protected, a dialog displays when you choose Administrator Settings.

  The IP network screen displays the H.323 settings, as shown next.

2 Configure the following H.323 settings:

- **Enable IP H.323** Check this option to enable IP H.323.
- **Display H.323 Extension** Check this option to enter H.323 extensions separately from the gateway ID on the Place a Call screen. If your system is registered with a gatekeeper, your H.323 extension displays on the home screen. If you do not check this option, you can make gateway calls by entering the call information in this format:
  `gateway ID + ## + extension`.
- **H.323 Name** Enter the name that gatekeepers and gateways use to identify this HDX system. You can make point-to-point calls using H.323 names if both systems are registered to a gatekeeper. The H.323 name is the same as the System Name, unless you change it. Note that your organization may use a dial plan that defines the names you can use. Note that your organization may use a dial plan that defines the names you can use.
- **H.323 Extension (E.164)** Entering an extension in this field enables you to place point-to-point calls if both systems are registered with a gatekeeper, and specifies the extension that gatekeepers and gateways use to identify this system.

- **Use Gatekeeper** A gatekeeper manages functions such as bandwidth control and admission control. The gatekeeper also handles address translation, which enables users to make calls using static aliases instead of IP addresses that may change each day. You can choose from the following options:
  - **Off** Calls do not use a gatekeeper. If you choose **Off**, the *Primary Gatekeeper IP Address* field is not displayed.
  - **Auto** This option causes the HDX system to attempt to automatically find an available gatekeeper.
  - **Specify** When you choose this option, calls you dial use the gatekeeper you specify in the Primary Gatekeeper field. You must choose Specify to enable H.235 Annex D Authentication.
  - **Specify with PIN** Choose this option to use the E.164 address you specify in the H.323 Extension (E.164) field. Calls you make using this option require an authentication PIN. Note that gateways and gatekeepers are required for calls between IP and ISDN.
- **Authentication** Check this option to enable support for H.235 Annex D Authentication. When you enable this option, the H.323 gatekeeper ensures that only trusted H.323 endpoints are allowed to access the gatekeeper. The following fields display when you enable Authentication:
  - **User Name** Specify the user name for authentication with H.235 Annex D.
  - **Password** Specify the password for authentication with H.235 Annex D.

- **Current Gatekeeper IP Address** This field is not configurable and displays the IP address that the HDX is currently registered to.
- **Primary Gatekeeper IP Address** The primary gatekeeper IP address contains the address with which the system registers. As part of the gatekeeper registration process, the gatekeeper might return alternate gatekeepers. If communication with the primary gatekeeper is lost, the HDX system registers with the alternate gatekeeper but continues to poll the primary gatekeeper. If the system reestablishes communications with the primary gatekeeper, the HDX system unregisters from the alternate gatekeeper and reregisters with the primary gatekeeper. Note that this field does not display if you chose *Off* in the *Use Gatekeeper* field.
  - If you chose to use an automatically selected gatekeeper, this field displays the gatekeeper's IP address.
  - If you chose to specify a gatekeeper, enter the gatekeeper's IP address or name (for example, `gatekeeper.companyname.usa.com`, or `10.11.12.13`).
- **Use PathNavigator for Multipoint Calls** Specify whether multipoint calls use the system's internal multipoint capability or the Conference on Demand feature available with Polycom PathNavigator™, ReadiManager® SE200, or Polycom CMA system. This feature is available only if the system is registered with one of these gatekeepers.

- **Alternate Gatekeepers** This field is not configurable and displays the alternative gatekeeper as a FQDN or by IP address.

Using Polycom's On Demand Conferencing Solution

Polycom's on demand conferencing solutions let you hold calls and conferences on the fly without making plans or reservations in advance. Polycom offers a number of collaboration solutions that enable rapid decision making and improved responsiveness. To find out more, see Polycom On Demand Conferencing Solution.

To place calls using on demand conferencing:

1. Register your Polycom HDX system with a Polycom gatekeeper. A Polycom RMX® system must be configured with the gatekeeper to provide the On Demand Conferencing solution.
2. Enable Use PathNavigator for Multipoint Calls.
3. Create a group in the directory (recommended).

When using On Demand Conferencing, once the call begins, you cannot add another site to the call — even if the site was in the call originally. Note that the Polycom RMX system must have enough ports available to complete the call.

- **Gateway** A gateway performs code and protocol conversion between H.323 (IP), SIP, and H.320 (ISDN), so that users on different networks can call one another. If you configure the HDX system to use a gateway, you must configure it to use a gatekeeper.
  - **Country Code** Specifies the country code for the system's location.
  - **Area Code** Specifies the area or city code for the system's location.
  - **Number** Specifies the extension that identifies this system for incoming gateway calls.
  - **Gateway Number Type** Use this field to change the default H.323 extension. Choose one of the following options:
    - **Number + Extension** Choose this option to have users dial in to the HDX system using the gateway number and HDX system extension number.
    - **Direct Inward Dial** Choose this option to have users dial in to an HDX system directly using an internal extension number. If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias.

Chapter 7: Integrating Polycom RMX Systems with Siemens OpenScape

This chapter shows you how to configure Polycom® RMX® 1500/2000/4000 systems and integrate the system with Siemens OpenScape® products. For more detailed information about configuring a Polycom RMX system, refer to the Polycom RMX documentation on the Polycom Support site.

Defining IP Network Services

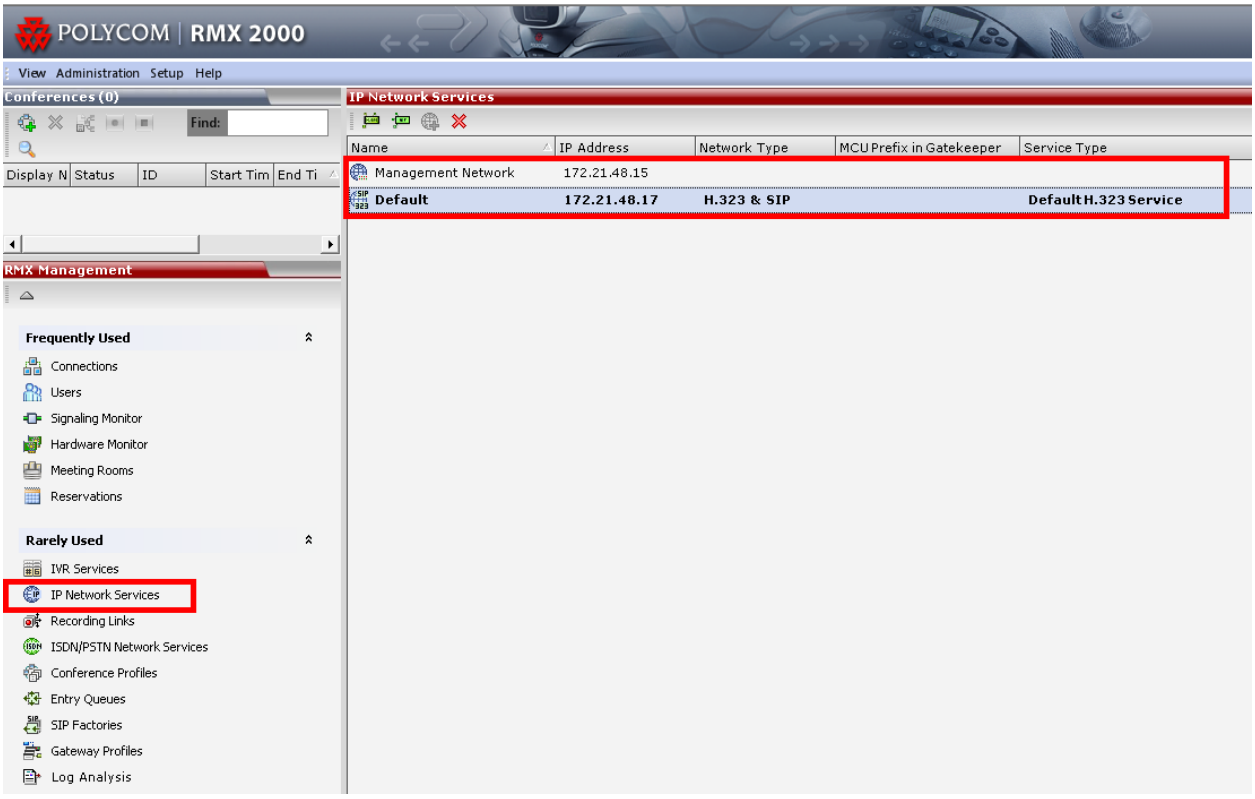
To enable the Polycom RMX system to function within the IP network environment, you need to define the network parameters for the IP Network Services. You can access the configuration dialog for the network services through the RMX Management pane of the RMX Web Client.

The Polycom RMX system uses two IP network services:

- Management Network
- Network Service (Conferencing Service)

  Both are shown in the following figure.

Figure 7-1: Management Network and Network Service



When using the RMX system with multiple services**,** you require five IP network services for the RMX 4000 and three IP network services for the RMX 2000 and RMX 1500.

Setting Mandatory System Flags

Next, you need to set mandatory system flags.

To set system flags:

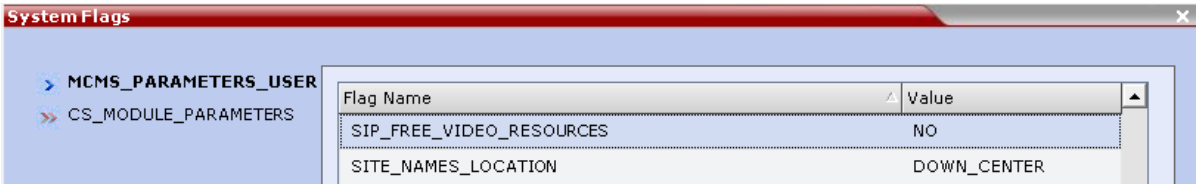
1 Navigate to **Setup > System Configuration**.

The System Flags dialog displays.

2 Set the following system flags:

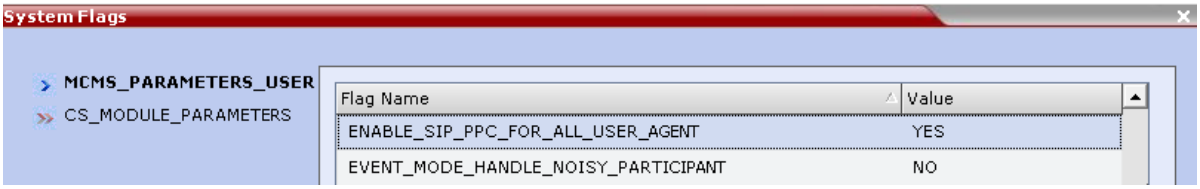
- SIP_FREE_VIDEO_RESOURCES NO

This setting is required because the OpenScape Desktop Client escalates from Audio to Video and is mandatory.



- ENABLE_SIP_PPC_FOR_ALL_USER_AGENT YES

This setting is required to enable Binary Floor Control Protocol (BFCP), which enables content over SIP, between the RMX system and the HDX system and is mandatory.



- ENABLE_FLOW_CONTROL_REINVITE NO

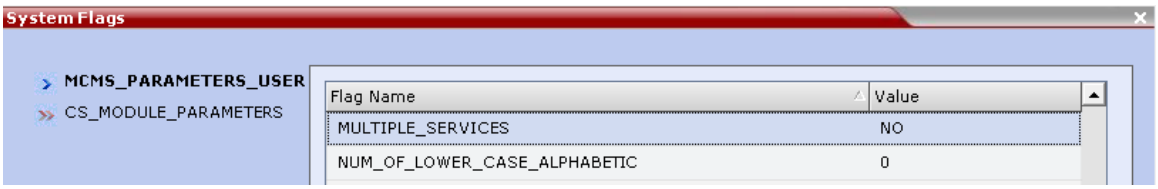
This flag is related to enable BFCP and is mandatory.

- ENABLE_H239 YES

This setting enables H239 and is mandatory.

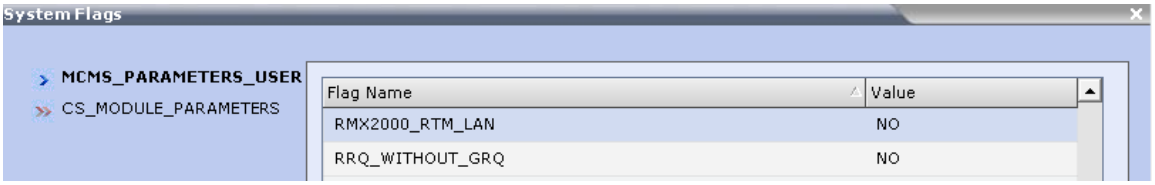
- MULTIPLE_SERVICES YES

This setting enables network separation and is only required if you use network separation.



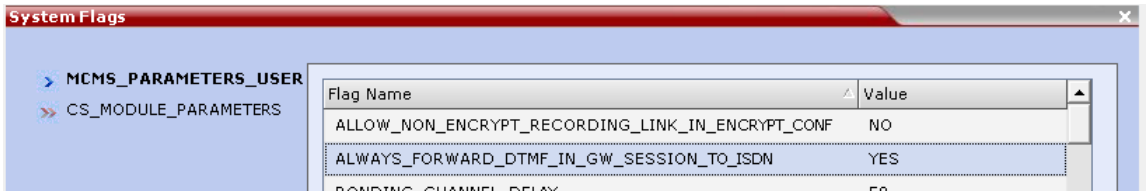
- RMX2000_RTM_LAN YES

This flag enables network separation using RTM LAN card for media and is only required when you use RTM LAN card.



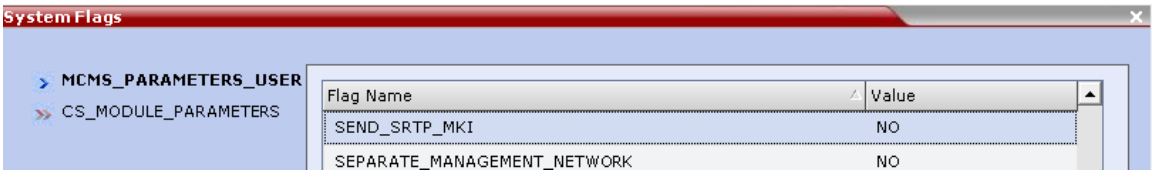
- ALWAYS_FORWARD_DTMF_IN_GW_SESSION_TO_ISDN YES

This setting allows you to send DTMF tones through an IP-ISDN gateway call and is mandatory if you use an IP-ISDN Gateway.



- SEND_SRTP_MKI NO

This setting is required and mandatory if you use TLS.



Creating a Primary Management Network

The primary Management Network is used to control the Polycom RMX system, primarily through the RMX Web Client application. The Management Network contains the network parameters, such as the IP address of the Control Unit, that are needed to connect the RMX and the RMX Web Client. The IP address can be used by the administrator or service personnel to connect to the Control Unit if the RMX system becomes corrupted or inaccessible.

You can create a private network the first time you power up the RMX system by using a USB key or a cable to set the Management Network parameters.

For more information, refer to the *Polycom RMX 1500/2000/4000 Administrator's Guide*.

Setting Up a Conferencing Network Service

You can use the Conferencing Network Service to configure and manage communications between the Polycom RMX system and conferencing devices such as endpoints, gatekeepers, SIP servers, and so forth.

The Network Service contains parameters for the following:

- Signaling Host IP Address
- MPM+ and MPMx boards (media processors)
- External conferencing devices

Calls you make from an external IP entity are made to the Signaling Host, which initiates call setup and assigns the call to the appropriate MPM + or MPMx board.

Conferencing definitions such as environment (H.323 or SIP) are also defined in this service.

Most of the Network Service is configured by the Fast Configuration Wizard, which runs automatically if the following occurs:

- First time power-up
- Deletion of the Network Service, followed by a system reset

Admin Tip: You Must Reset the RMX System to Apply Changes

Changes made to any of these parameters take effect after you have reset the Polycom RMX unit. An active alarm is created when changes you have made to the system have not yet been implemented, which indicates that the MCU must be reset.

Modifying the Management Network Service

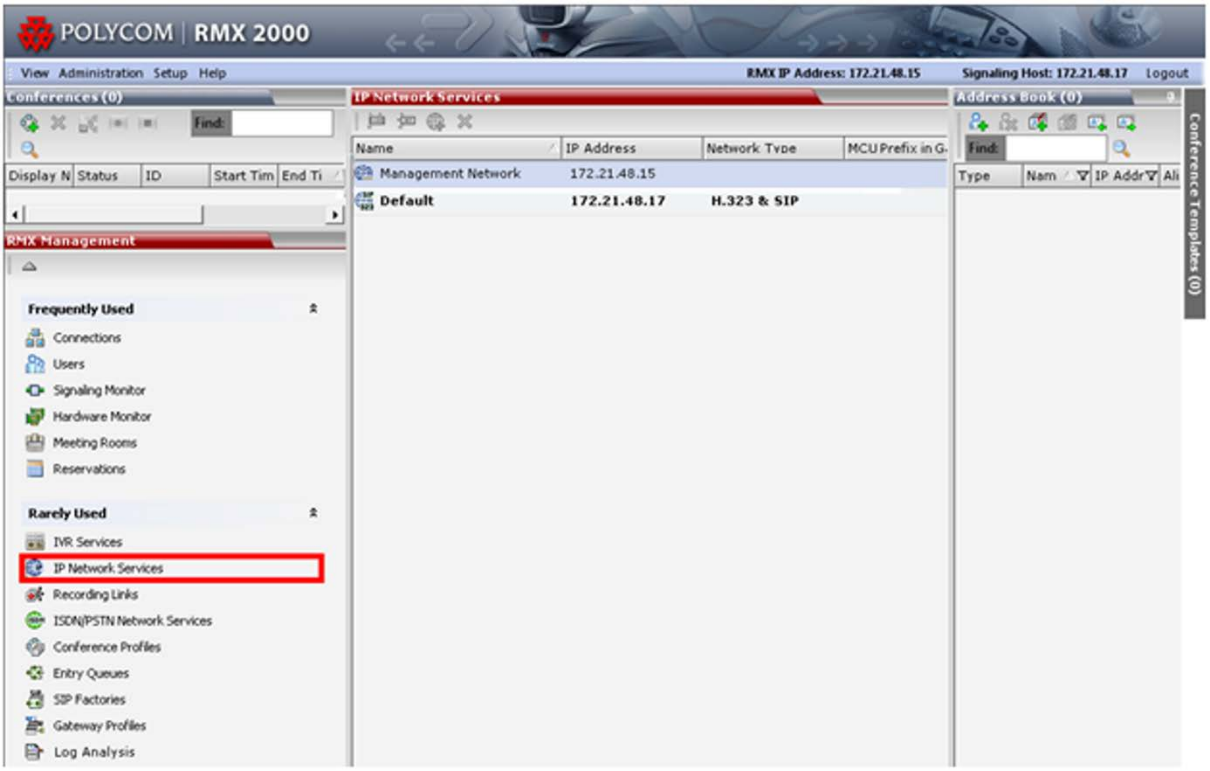
You must modify the Management Network parameters to perform the following tasks:

- Connect directly to the RMX system from a workstation
- Modify routes
- Modify DNS information

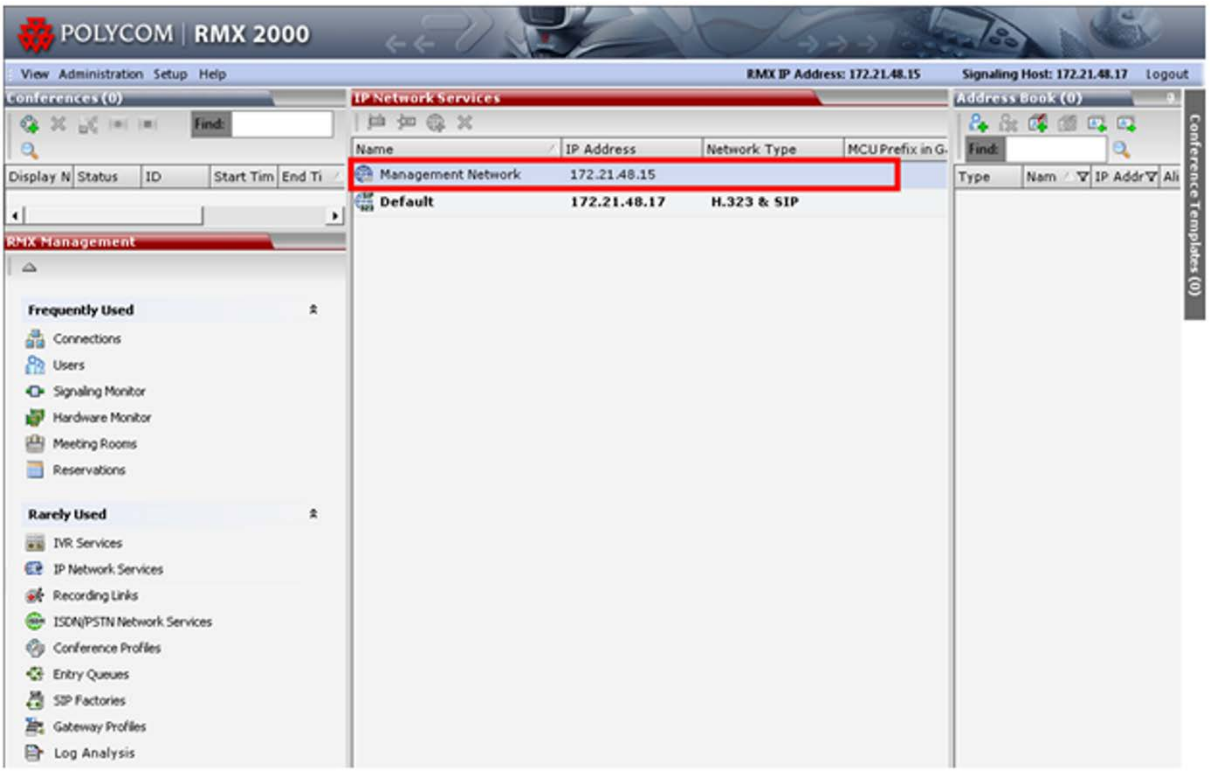
You can configure the Management Network H.323 settings using the system user interface or the web interface. This procedure shows you how to configure settings using the web interface.

To view or modify the Management Network Service:

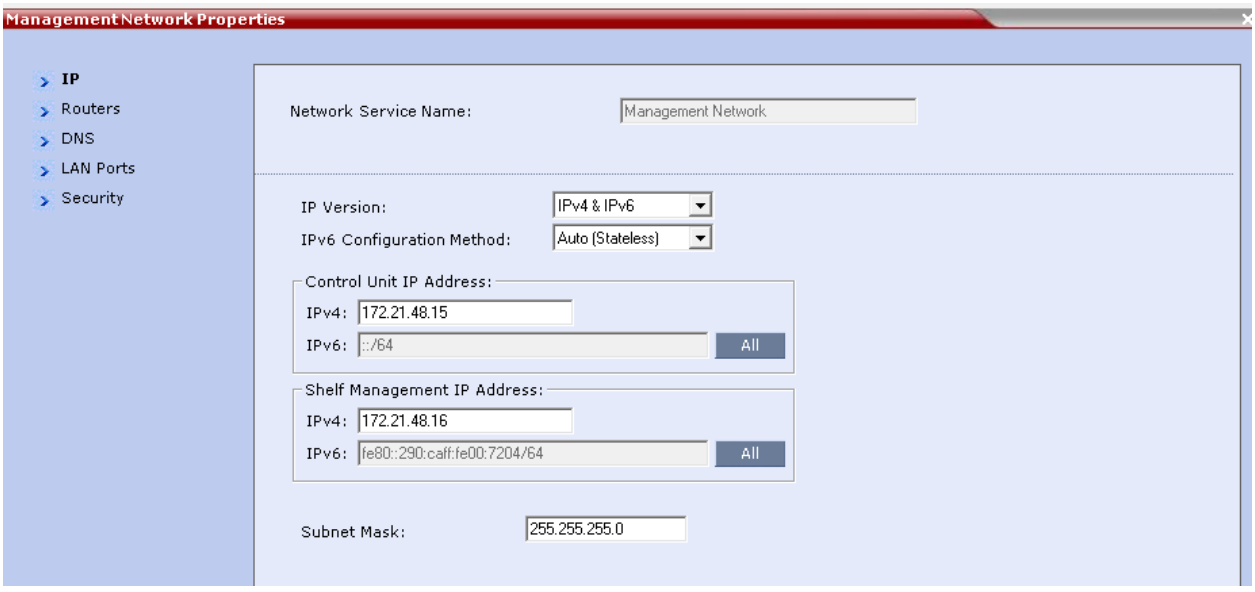
1 In the RMX Management pane, choose **IP Network Services**, shown next.



2 In the IP Network Services screen, choose **Management Network**, shown next.



The IP Network Services screen displays, shown next.



3 Modify the following fields:

- **Network Service Name** This field displays the name of the management network. You cannot modify this name. Note that this field displays in all Management Network Properties tabs.

- **IP Version** Choose one of the following versions:
  - **IPv4** Select this option for IPv4 addressing only.
  - **IPv6** Select this option for IPv6 addressing only.
  - **IPv4 & IPv6** Select this option for both IPv4 and IPv6 addressing.
- **IPv6 Configuration Method** Choose Auto (Stateless) or Manual.

  If you choose *Auto*, the following address are generated:
  - Link-Local (For internal use only)
  - Site-Local
  - Global

If you choose *Manual*, you can manually enter the following addresses:

- Site-Local
- Global

You cannot manually modify the following address types:

- Link-Local
- Multicast
- Anycast

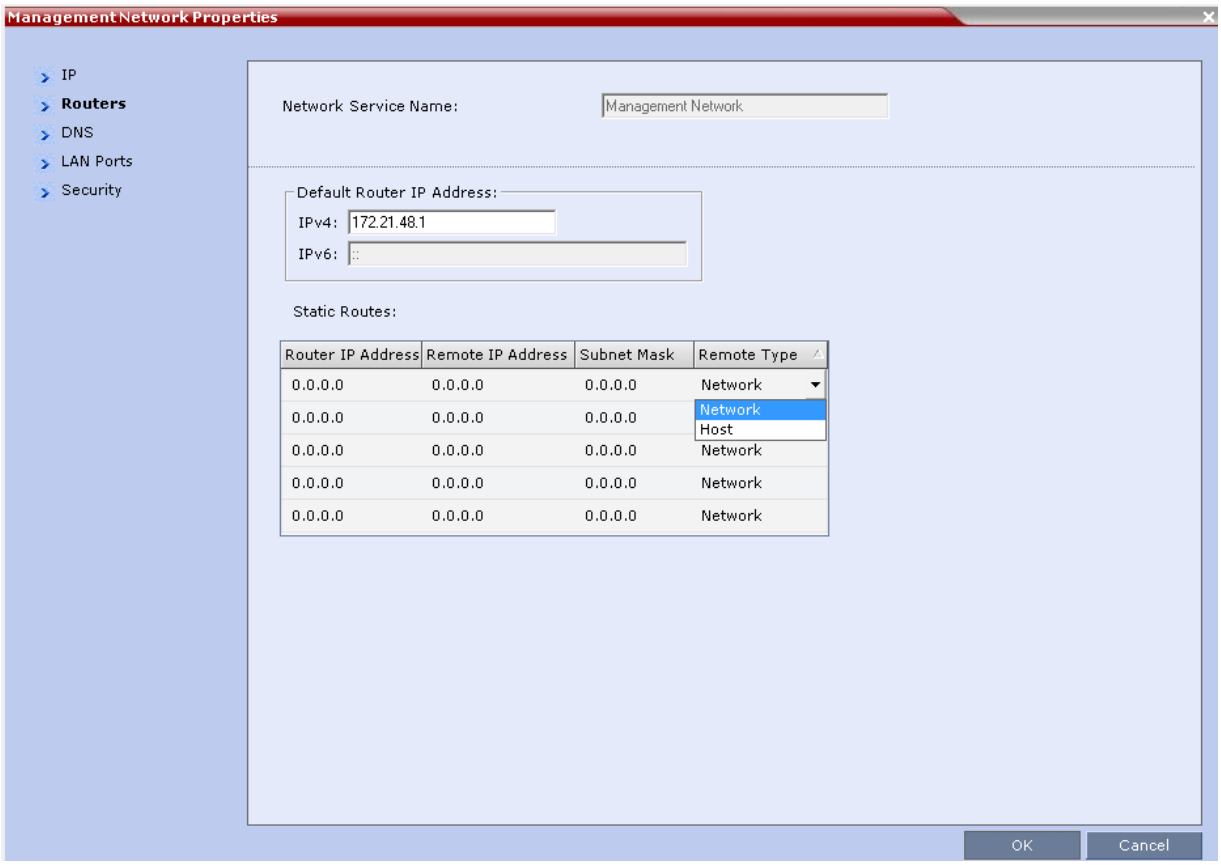
- **Shelf Management IP Address** Enter an IPv4 or IPv6 IP address for the RMX Shelf Management Server. The IPv4 address of the RMX Shelf Management Server is used by the RMX Web Client to monitor hardware. The IPv6 address of the RMX Shelf Management Server is used by the RMX Web Client to monitor hardware. Note that you must use Internet Explorer 7™ to connect to the RMX Web Client to the RMX using IPv6.

Click the **All** button to display the IPv6 addresses as follows:

- **Auto** If selected, Site-Local and Global site addresses are displayed.
- **Manual** If selected, only the Manual site address is displayed.

- **Subnet Mask** Enter the subnet mask of the Control Unit. Note that this field is specific to IPv4 and is not displayed in IPv6 only mode.

4 Click **Routers**, shown next, and modify the following fields:



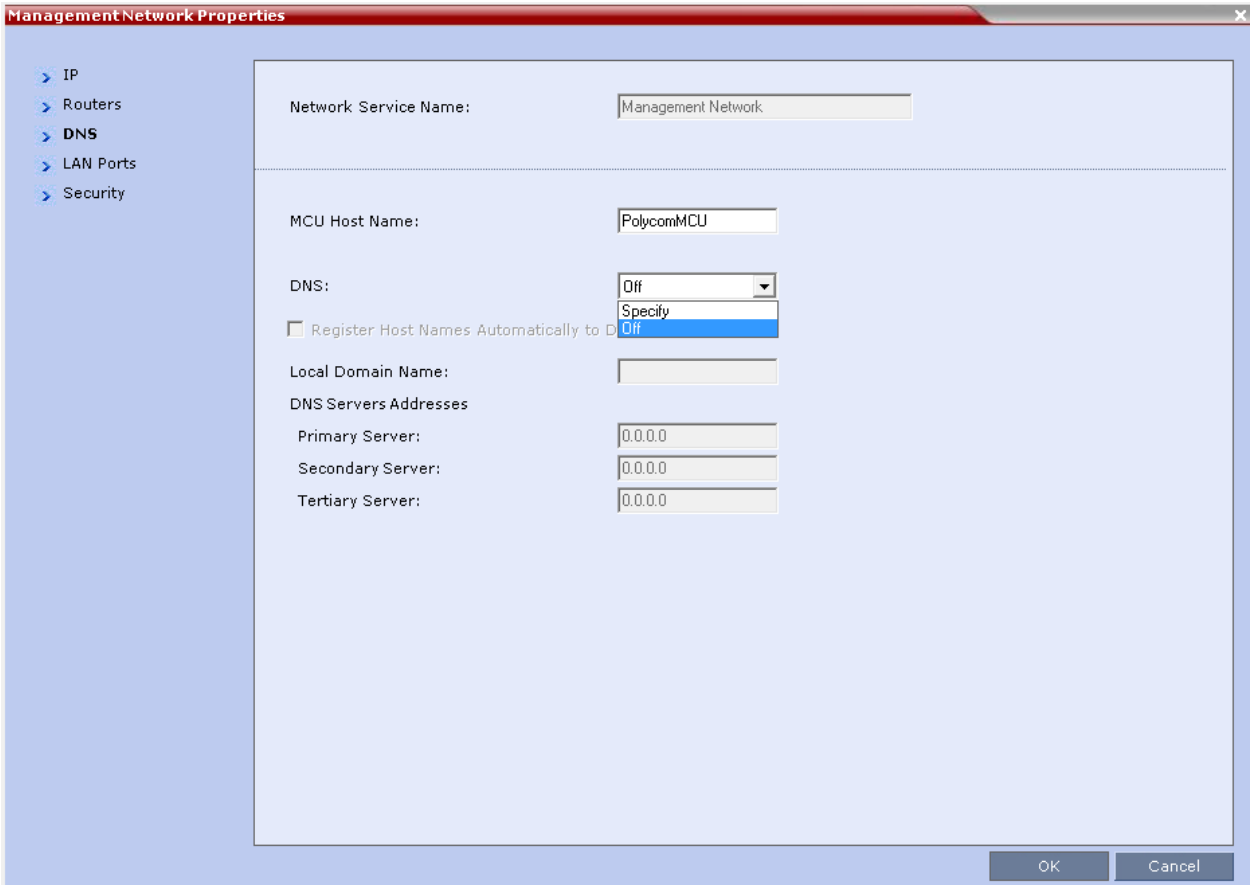
- **Default Router IP Address** Enter an IPv4 or IPv6 IP address for the default router. The default router is used whenever the defined static routers are unable to route packets to their destination. The default router is also used when host access is restricted to one default router.
- **Static Routes IPv4 Only Table** The system uses Static Routes to search other networks for endpoint addresses that are not found on the local LAN. You can define up to five routers in addition to the default router. The order in which the routers display in the list determines the order in which the system looks for the endpoints on the various networks. If the address is in the local subnet, no router is used. To define a static route (starting with the first one), click the appropriate column and enter the required value. Enter values for the following options:
- **Router IP Address** Enter the IP address of the router.
- **Remote IP Address** Enter the IP address of the entity to be reached outside the local network. The Remote Type determines whether this entity is a specific component (Host) or a network.

  If Host is selected in the Remote Type field, enter the IP address of the endpoint.

  If Network is selected in the Remote Type field, enter of the segment of the other network.
- **Remote Subnet Mask** Enter the subnet mask of the remote network.

- **Static Routes IPv4 Only Table** Select the type of router connection:
  - **Network** Defines a connection to a router segment in another network.
  - **Host** Defines a direct connection to an endpoint found on another network.

5 Choose **DNS** and modify the following fields:



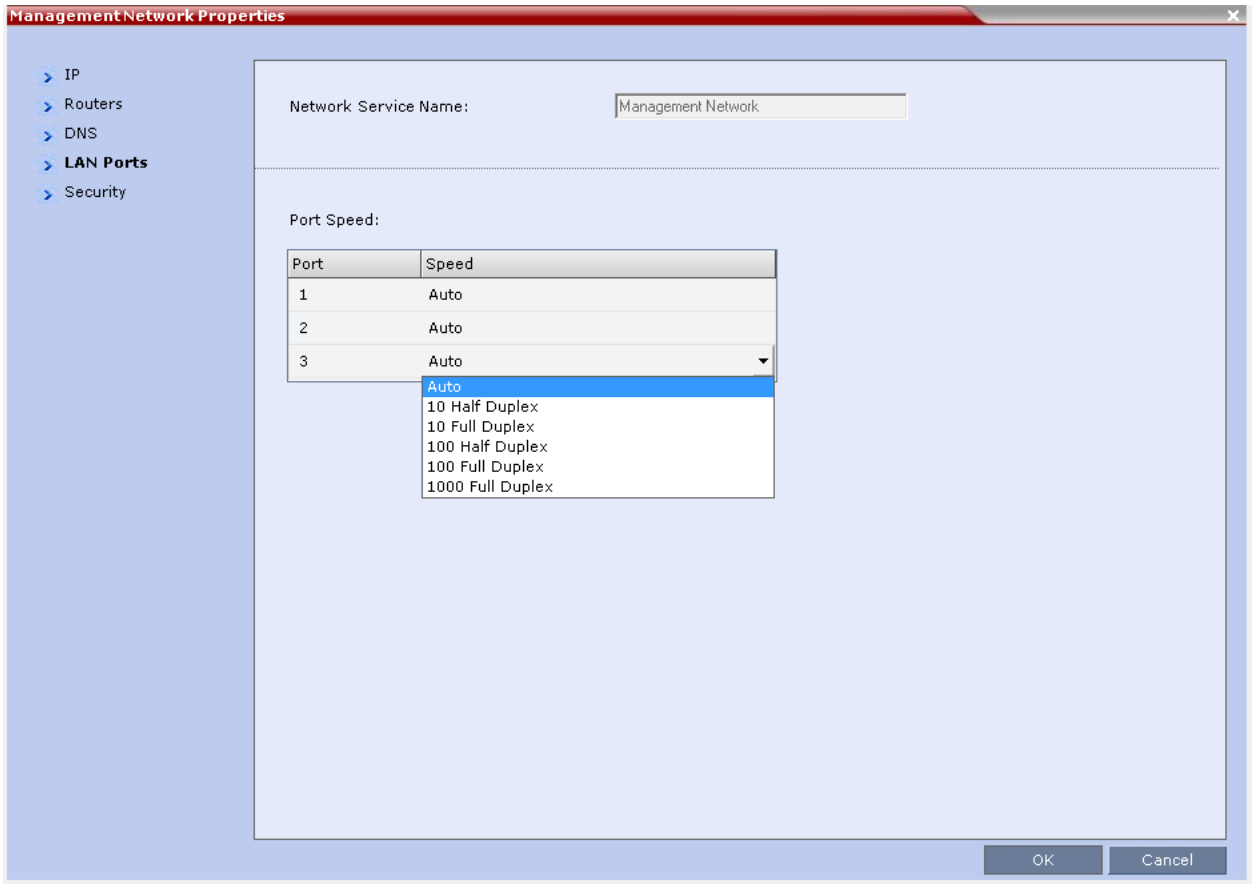
- **MCU Host Name** Enter the name of the MCU on the network. The default name is RMX.
- **DNS** Choose from one of the following options:
  - **Off** DNS servers are not used in the network.
  - **Specify** Enter the IP addresses of the DNS servers. Note that this field must be enabled to make the P address fields available.

- **Register Host Names Automatically to DNS Servers** Select this option to automatically register the MCU Signaling Host and Shelf Management with the DNS server.
- **Local Domain Name** Enter the name of the domain where the MCU is installed.
- **DNS Servers Addresses** You can define address for the following servers up to a maximum of three servers:
  - Primary Server

» Secondary Server

» Tertiary Server

6 If you are using an RMX 2000, choose **LAN Ports** and modify the following fields:



Admin Tip: Configuring RMX 1500/4000 and RMX 2000 LAN Port Modes

When configuring the RMX 1500/4000 platforms, you can manually modify automatically identified speed and transmit/receive mode for each LAN port that the system uses if required by the specific switch in the Ethernet Settings dialog.

- **Port Speed** You can set the speed and transmit/receive mode manually for LAN 2 Port only. Do not change the automatic setting of Port 1 and Port 3. Any change to the Port 1 speed will not be applied.
- **Port** Choose port 1, 2, or 3

- **Speed** Choose the speed and transmit/receive mode for each port. The default setting is Auto which starts at 1000 Mbps Full Duplex, proceeding downward to 10 Mbps Half Duplex. To maximize conferencing performance, especially in high bit rate call environments, use a 1Gb connection.

7 Click **OK**. If you have modified the Management Network Properties, reset the MCU.

Modifying the Network Service

The Network Service parameters need to be modified if you want to change any of the following:

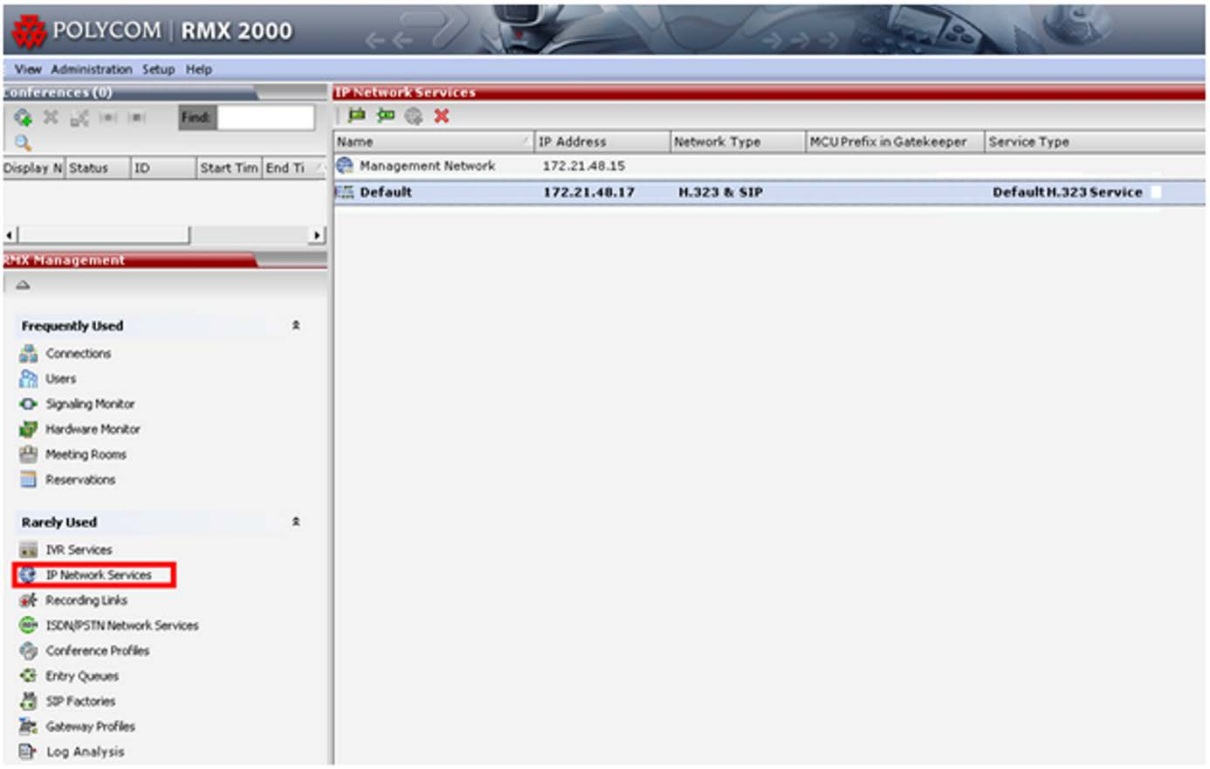
- The network type that the RMX connects to
- The IP address of the RMX Signaling Host
- The IP addresses of the RMX Media boards
- The subnet mask of the RMX's IP cards
- The gatekeeper parameters, including additional gatekeepers you want to add to the Alternate Gatekeepers list
- SIP server parameters

Configuring RMX IP Settings

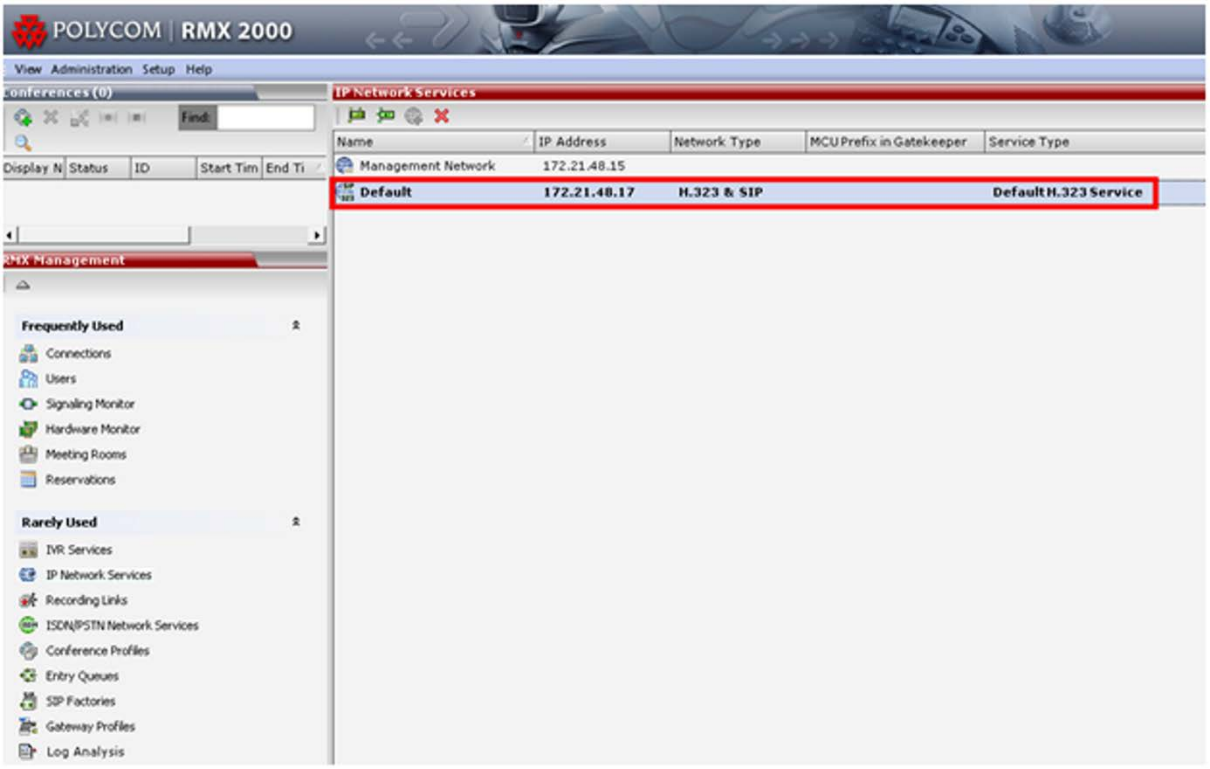
This section shows you how to configure RMX IP Settings.

To view or modify the Network Service:

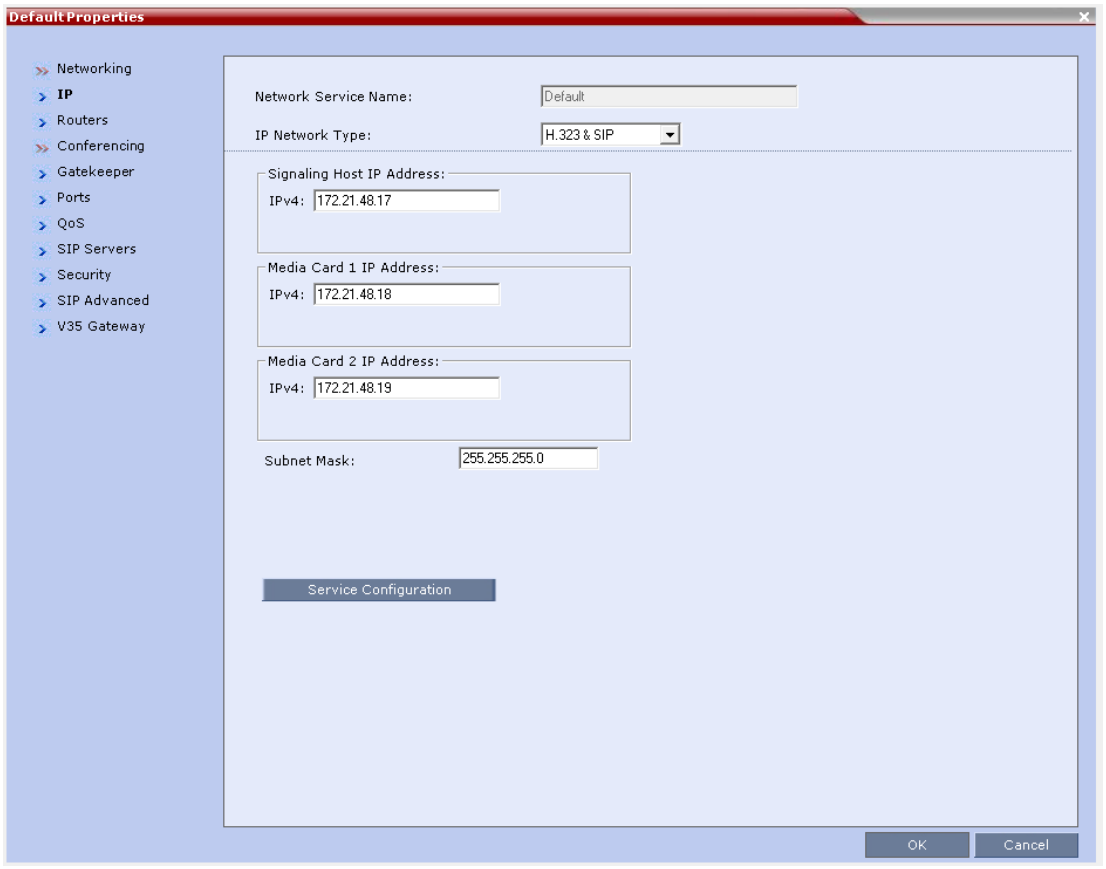
1 In the RMX Management pane, choose **IP Network Services**, shown next.



2 In the IP Network Services screen, choose **Default**, shown next. Note that *Default* refers to the default network service.



The Default Properties screen displays the default network service settings.



3 Modify the following fields:

- **Network Service Name** Enter the name of the IP network service. The Fast Configuration Wizard assigns *Default IP Service* as the default value in the Network Service Name field.
- **IP Network Type** Displays the network type selected the first time you enter configured this field. The Default IP Network icon indicates the selected environment. Choose from the following options:
  - » **H.323** For an H.323-only Network Service.
  - » **SIP** For a SIP-only Network Service.
  - » **H.323 & SIP** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this service.

Note: Field Availability

The IP Network Type field is displayed in all Network Service tabs.

- **Signaling Host IP Address** Enter the address you want IP endpoints to use when dialing in to the MCU. Dial out calls from the RMX system are initiated from this address. This address is used to register the RMX system with a Gatekeeper or a SIP Proxy server.
- **Media Card 1 Port 1 IP Address** and **Media Card 1 Port 2 IP Address (RMX 4000)** If only one network is connected to this media card, it is enough to assign one media card to this Network Service. In such a case, enter one IP address for the media card according to the LAN Port used for the connection.

  If each of the LAN ports on one media card is used with two different networks, each port is assigned to its own Network Service. In such a case, enter the IP address of the port to be assigned to this Network Service.

  A LAN port that is already assigned to a different Network Service, displays the IP Address of the assigned port and it cannot be assigned to this Network Service (it is disabled).
- **Media Card 2 Port 1 IP Address (RMX 2000/4000)** and **Media Card 2 Port 2 IP Address** (RMX 4000) Enter the IP address(es) of the media card(s) as provided by the network administrator:
- RMX1500: MPMx 1
- RMX 2000: MPM+/MPMx 1 and MPM+/MPMx 2 (if installed)
- RMX 4000: MPM+/MPMx 1, MPM+/MPMx 2 (if installed), MPM+/MPMx 32 (if installed) and MPM+/MPMx 4 (if installed)

The media card uses these addresses to connect to conferences and transmit call media, including video, voice, and content.

- Subnet **Mask** Enter the subnet mask of the MCU. The default value is `255.255.255.0`.

Configuring RMX Routers

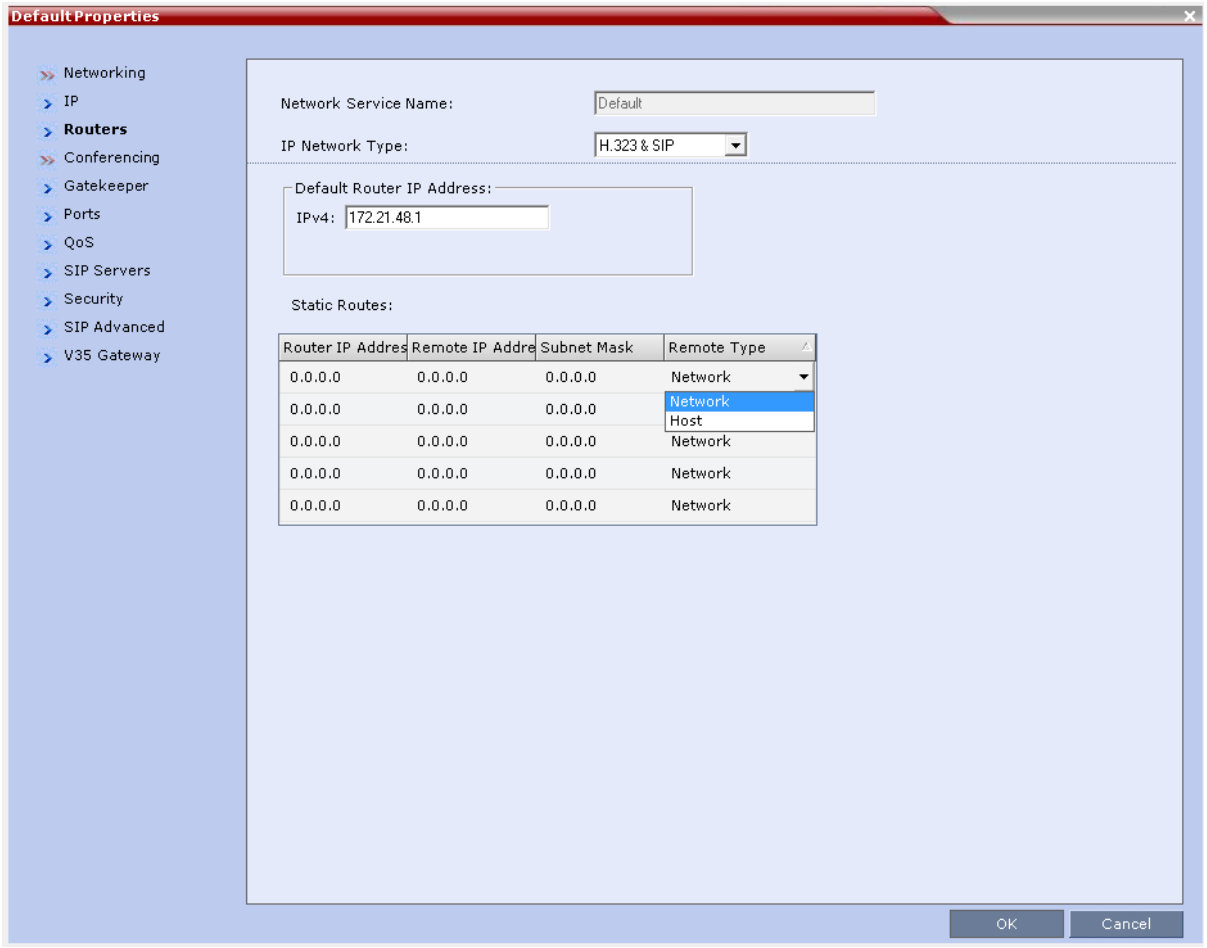
This section shows you how to configure router settings for the RMX.

To configure router settings:

1 In the RMX Management pane, click **Routers**.

The Routers settings display, shown next.

With the exception of **IP Network Type**, the field definitions of the *Routers* tab are the same those shown in Network Service.



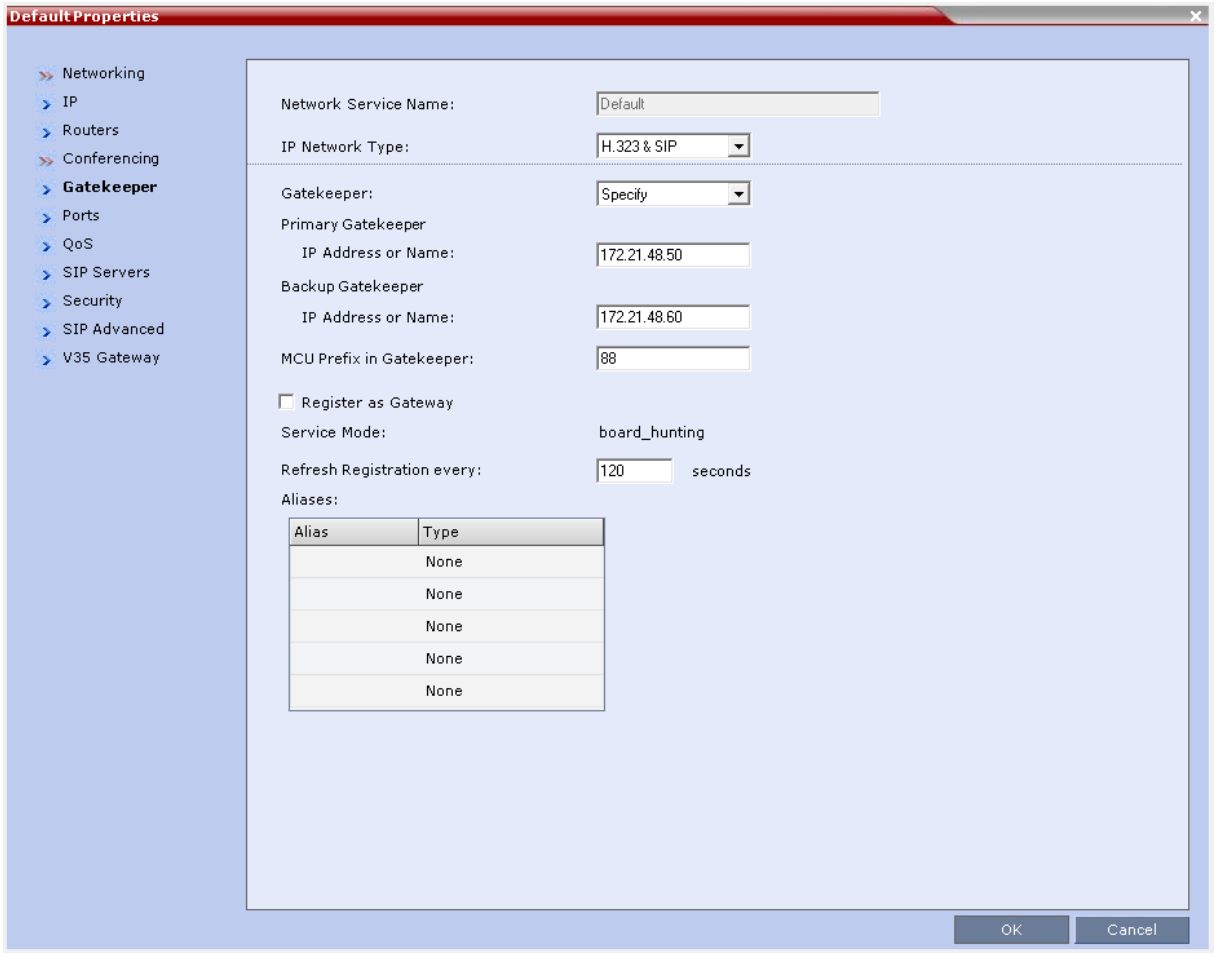
Configuring Gatekeeper Settings

This section shows you how to configure gatekeeper settings.

To configure gatekeeper settings:

1 Click the **Gatekeeper** Tab.

The Gatekeeper settings display, as shown next.



2 Modify the following fields:

- **Gatekeeper** Choose one of the following options:
  - » **Specify** Enables configuration of the gatekeeper IP address.
  - » **Off** Disables all gatekeeper options.
- **Primary Gatekeeper** Enter an IP Address or the gatekeeper's host name registered in the DNS.

Admin Tip: Use a Hostname in IPv4 & IPv6 or IPv6 Mode

When in IPv4 & IPv6 or in IPv6 mode, it is easier to use a hostname instead of an IP address.

- **Backup Gatekeeper** Enter an IP Address or the DNS host name or IP address of the gatekeeper used as a fallback gatekeeper used when the primary gatekeeper is not functioning properly.

- **MCU Prefix in Gatekeeper** Enter the number that the Network Service registers with in the gatekeeper. H.323 endpoints use this number as the first part of their dial-in string when dialing the MCU. Note that when you use PathNavigator SE200, this prefix automatically registers with the gatekeeper. When another gatekeeper is used, this prefix must also be defined in the gatekeeper.
- **Register as Gateway** Select this option if you want to use the RMX unit as a gateway, for example, when you are using an alternate gatekeeper.
- **Refresh Registration every __ seconds** Specify an interval of time that the RMX system informs the gatekeeper that it is active. The RMX system re-sends the IP address and aliases of the IP cards to the gatekeeper. If the IP card does not register within the defined time interval, the gatekeeper will not refer calls to this IP card until it re-registers. If set to 0, re-registration is disabled. Polycom recommends using default settings. This is a re-registration and not a keep-alive operation – an alternate gatekeeper address may be returned.
- **Aliases** You can specify an alias and a type.
- **Alias** Enter an alias that identifies the RMX's Signaling Host within the network. Up to five aliases can be defined for each RMX.

Note: Enter a Prefix for Each Gatekeeper

When you specify a gatekeeper, you must enter at least one prefix or alias in the table.

- Type The type defines the format in which the card's alias is sent to the gatekeeper. You can specify the following types of alias:
  - H.323 ID (alphanumeric ID)
  - E.164 (digits 0-9, * and #)
  - Email ID (email address format, for example, abc@example.com)
  - Participant Number (digits 0 to 9, *, and #)

Admin Tip: Using Alias Types

Although all alias types are supported, the type of alias you use depends on the gatekeeper's capabilities.

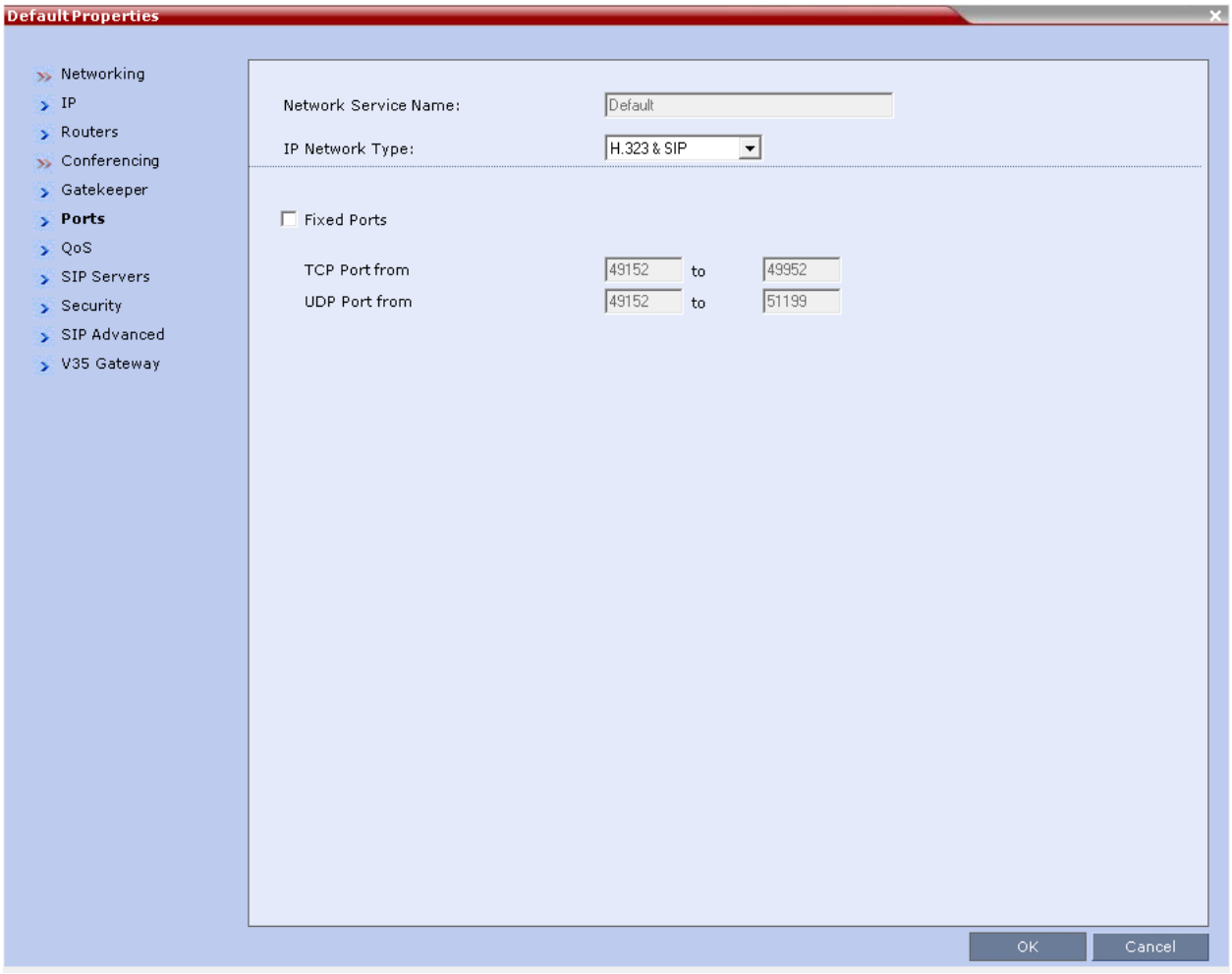
Configuring Ports

Settings in the Ports tab allow you to allocate specific ports in the firewall to multimedia conference calls. The port range recommended by the Internet Assigned Numbers Authority (IANA) is 49152 to 65535. The MCU uses this recommendation along with the number of licensed ports to calculate the port range.

To configure ports:

1 Click **Ports**.

The Ports settings display, shown next.



2 Modify the following fields:

- **Fixed Ports** Check this option to manually define the port ranges or to limit the number of ports to be left open. Leave this option cleared if you are defining a Network Service for local calls that do not require configuring the firewall to accept calls from external entities. When cleared, the system uses the default port range and allocates 4 RTP and 4 RTCP ports for media channels (Audio, Video, Content and FECC).

Note: Enabling ICE

When ICE Environment is enabled, eight additional ports are allocated to each call.

- **TCP Port from_to_** These fields display the default settings for port numbers used for signaling and control. To modify the number of TCP ports, enter the first and last port numbers in the range. The number of ports is calculated as follows: Number of simultaneous calls x 2 ports (1 signaling + 1 control).
- **UDP Port from_to_** These fields display the default settings for port numbers used for audio and video.
  - » To modify the number of UDP ports in Card Configuration Mode, enter the first and last port numbers in the range. The number of ports is calculated as follows:

    Number of simultaneous calls x 8 ports (2 audio, 2 video, 2 Content, and 2 FECC).
  - » To modify the number of UDP ports in MPM+/MPMx Card Configuration Mode, enter the first and last port numbers in the range, and the range must be 1024 ports. When ICE environment is enabled, the range must be 2048 ports.

Caution: Specifying Port Ranges

If you do not specify an adequate port range, the system accepts the settings and issues a warning. Calls are rejected when the MCU's ports are exceeded.

Configuring QoS Settings

This section shows you how to configure Quality of Service (QoS) settings in the RMX Management pane. QoS is important when transmitting high bandwidth audio and video information. The following QoS features can be measured and guaranteed:

- Average delay between packets
- Variation in delay (jitter)

- Transmission error rate

The RMX system supports two QoS methods: DiffServ and IP Precedence. Each method uses a different way to encode packet priority in the packet header. The RMX system implements QoS per Network Service, not per endpoint.

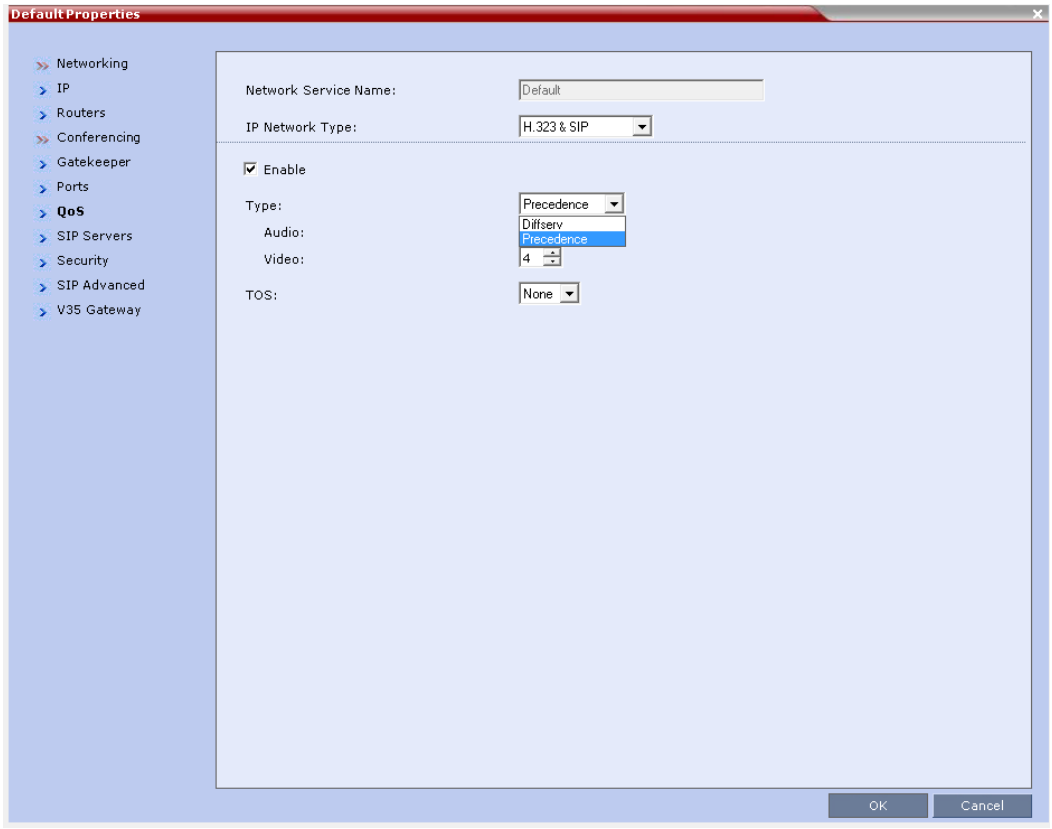
Note: The Routers Must Support QoS

Note that the routers must support QoS to allow IP packets to get higher priority.

To configure QoS settings:

1 In the RMX Management pane, click **QoS**.

The QoS settings display, as shown next.



Admin Tip: Routers Must Support QoS

The routers must support QoS in order for IP packets to get higher priority.

2 Modify the following fields:

- **Enable** Check this option to enable the configuration and use of the QoS settings. When un-checked, the values of the Differentiated Services Code Point (DSCP) bits in the IP packet headers are zero.
- **Type** Choose a method for encoding packet priority. The priority you set here for audio and video packets must match the priority set in the router. You can choose from the following options:
  - **DiffServ** Choose this option when the network router uses DiffServ for priority encoding. The default priority for both audio and video packets is 0x88. These values are determined by the QOS_IP_VIDEO and QOS_IP_AUDIO flags in the system.cfg file.
  - **Precedence** This is the default mode and is capable of providing priority services to all types of routers, as well as being currently the most common mechanism. Use this option when the network router uses Precedence for priority encoding, or when you are not sure which method is used by the router. Precedence needs to be combined with None in the TOS field. The default priority is 5 for audio and 4 for video packets.

  Audio / Video You can prioritize audio and video IP packets to ensure that all participants in the conference hear and see each other clearly. Choose a scale from 0 to 5, where 0 is the lowest priority and 5 is the highest. The recommended priority is 4 for audio and 4 for video to ensure that the delay for both packet types is the same and that audio and video packets are synchronized and to ensure lip sync.
- **TOS** Choose the type of service (TOS) that defines optimization tagging for routing the conferences' audio and video packets. Choose from the following options:
  - **Delay** The recommended option for video conferencing. Prioritized audio and video packets tagged with this definition are delivered with minimal delay because the throughput of IP packets minimizes the queue sequence and the delay between packets.
  - **None** No optimization definition is applied. This is a compatibility mode in which routing is based on Precedence priority settings only. Select None if you do not know which standard your router supports.

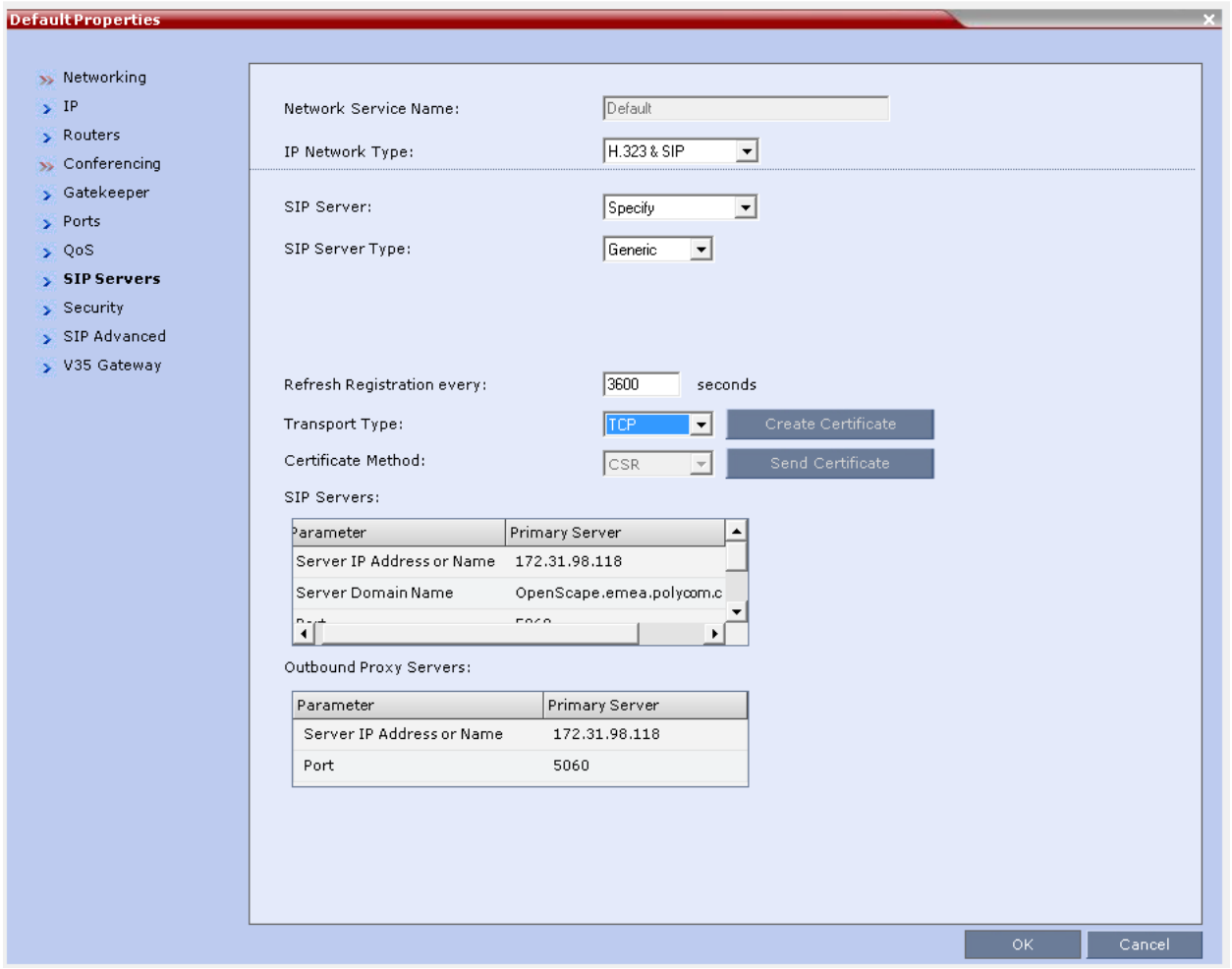
Configuring the SIP Servers

This section shows you how to configure the RMX to connect to the SIP server.

To configure the RMX to connect to the SIP server:

1 Click **SIP Servers**.

The SIP Servers settings display, shown next.

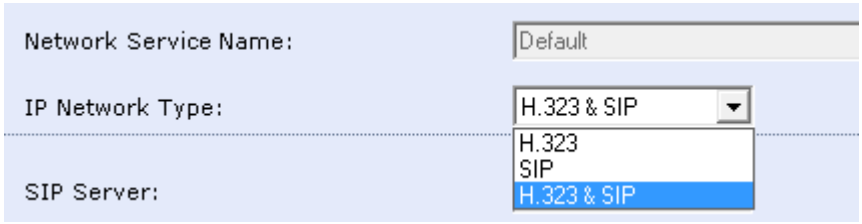


Note: You can use Unicode encoding in all SIP Signaling Dialogs.

You can use Unicode encoding and character sets that use Unicode encoding for all SIP Signaling settings.

2 Modify the following fields:

- **IP Network Type** Displays the network type selected the first time you enter configured this field. The Default IP Network icon indicates the selected environment. Choose from the following options:

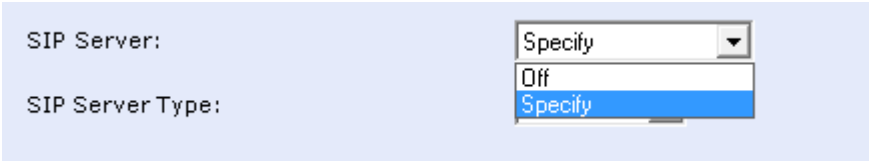


» **H.323** For an H.323-only Network Service.

» **SIP** For a SIP-only Network Service.

» **H.323 & SIP** For an integrated IP Service. Both H.323 and SIP participants can connect to the MCU using this option.

○ **SIP Server** Use the default value Specify.

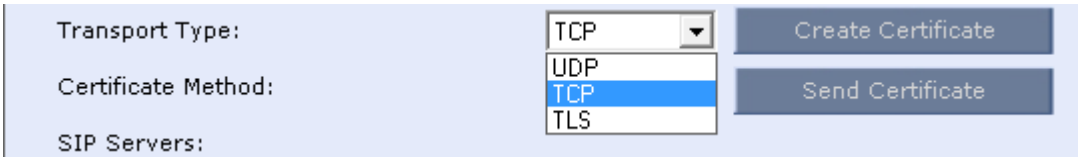


○ **SIP Server Type** Choose one of the following options:

» **Generic** Choose Generic.

○ **Refresh Registration every** The time that an inactive RMX will re-register with OpenScape Voice. The default value is 3600 seconds

○ **Transport Type** Three options display in the drop-down menu:

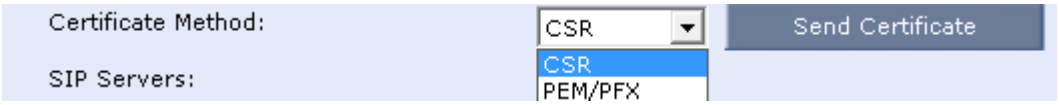


» **UDP** This option is not supported in this environment.

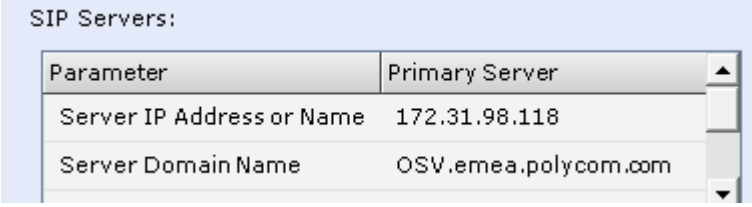
» **TCP** Choose this option for standard communication.

» **TLS** Choose this option if you are using secure communications.

○ **Certificate Method** This option is available only if you choose TLS in the Transport Type field.



- **SIP Servers** You can use one or more primary or alternate servers.



» **Server IP Address or Name** *S*IP IP address or FQDN of the OpenScape Voice**.** Enter the IP address of the *p*referred SIP server.

Admin Tip: Use a Hostname in IPv4 & IPv6 or IPv6 Mode

When in IPv4 & IPv6 or in IPv6 mode, it is easier to use Names instead of IP addresses.

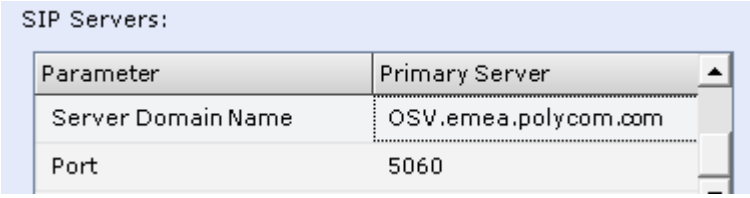
» **Server Domain Name** SIP IP address or FQDN of the OpenScape Voice

Enter the name of the domain that you are using for conferences, for example: `user_name@domain name` .

The domain name is used for identifying the SIP server in the appropriate domain according to the host part in the dialed string.

For example, when a call to `EQ1@polycom.com` reaches its outbound proxy, this proxy looks for the SIP server in the `polycom.com` domain, to which it will forward the call.

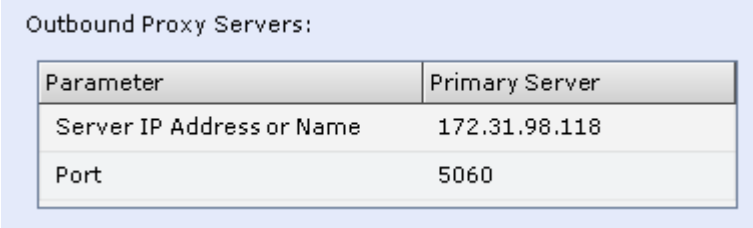
When this call arrives at the SIP server in `polycom.com`, the server looks for the registered user (EQ1) and forwards the call to this Entry Queue or conference.



» **Port: 5060** Enter the number of the TCP or TLS port used for listening. The port number must match the port number configured in the SIP server.

The default TCP port is 5060. The default TLS port is 5061.

- **Outbound Proxy Servers** Primary / Alternate Server Parameter


Outbound Proxy Servers:

Parameter	Primary Server
Server IP Address or Name	172.31.98.118
Port	5060

Server IP Address or Name Enter the SIP IP address or Fully Qualified Domain Name (FQDN) of OpenScape Voice. By default, the Outbound Proxy Server is the same as the SIP Server. If they differ, modify the IP address of the Outbound Proxy and the listening port number**.**

Port: 5060 Enter the port number that the outbound proxy is listening to. The default port for TCP is 5060 and for TLS 5061

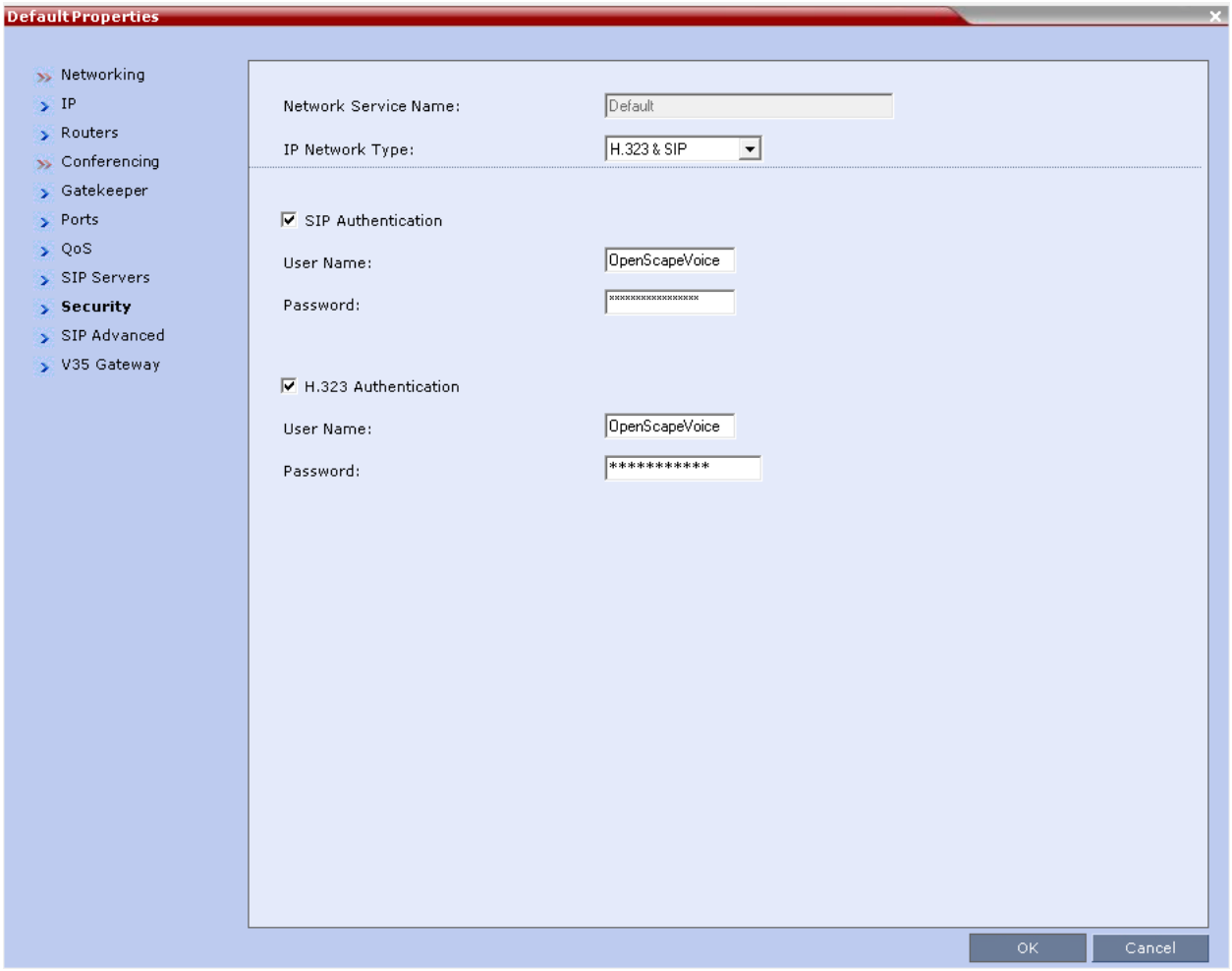
Configuring Security Settings

This section shows you how to configure security settings for the RMX.

To configure security settings:

1 Click **Security**.

The Security settings display, shown next.



2 Modify the following fields:

- **Authentication User Name** Enter the conference, entry queue, or meeting room name that is registered with the proxy. This field can contain up to 20 ASCII characters.
- **Authentication Password** Enter the conference, entry queue, or meeting room password as defined in the proxy. This field can contain up to 20 ASCII characters.

Admin Tip: Register the RMX as a Trusted Entity

If you leave the Authentication User Name and Authentication Password fields empty, the SIP digest authentication request is rejected. For registration without authentication, you must register the RMX system as a trusted entity on the SIP server.

Modifying Ethernet Settings

When using the RMX 1500/4000 platforms, you can manually modify the automatically identified speed and transmit/receive mode of each LAN port that the system uses if the specific switch requires it in the Ethernet Settings dialog.

Admin Tip: RMX 1500 Dialog Port Numbers and RMX 1500 MCU Port Numbers are Different

The port numbers displayed on the RMX 1500 dialog do not reflect the physical port numbers that labeled on the RMX 1500 MCU.

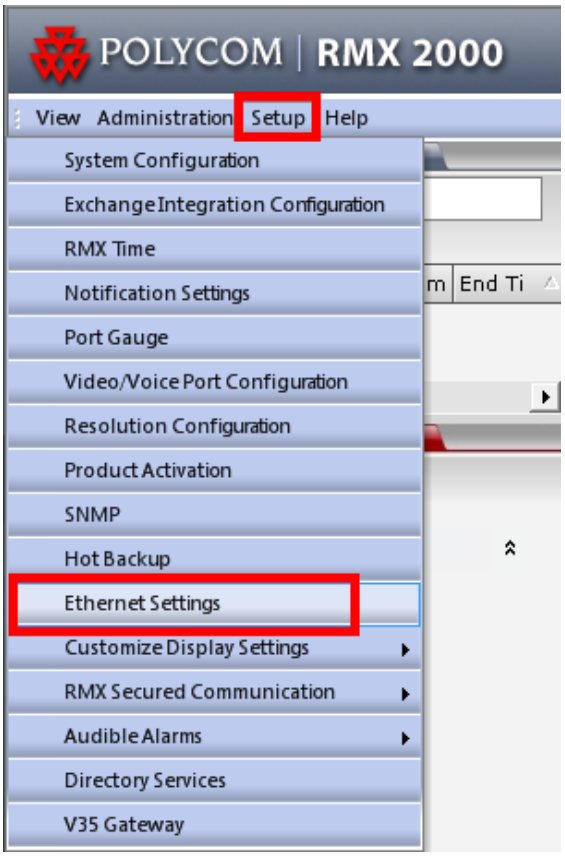
You will need to match the port type to the label on the back panel of the RMX 1500 MCU. Use the following table to match the port type to the back panel label.

Table 7-1: Matching Port Type to Label on the RMX 1500

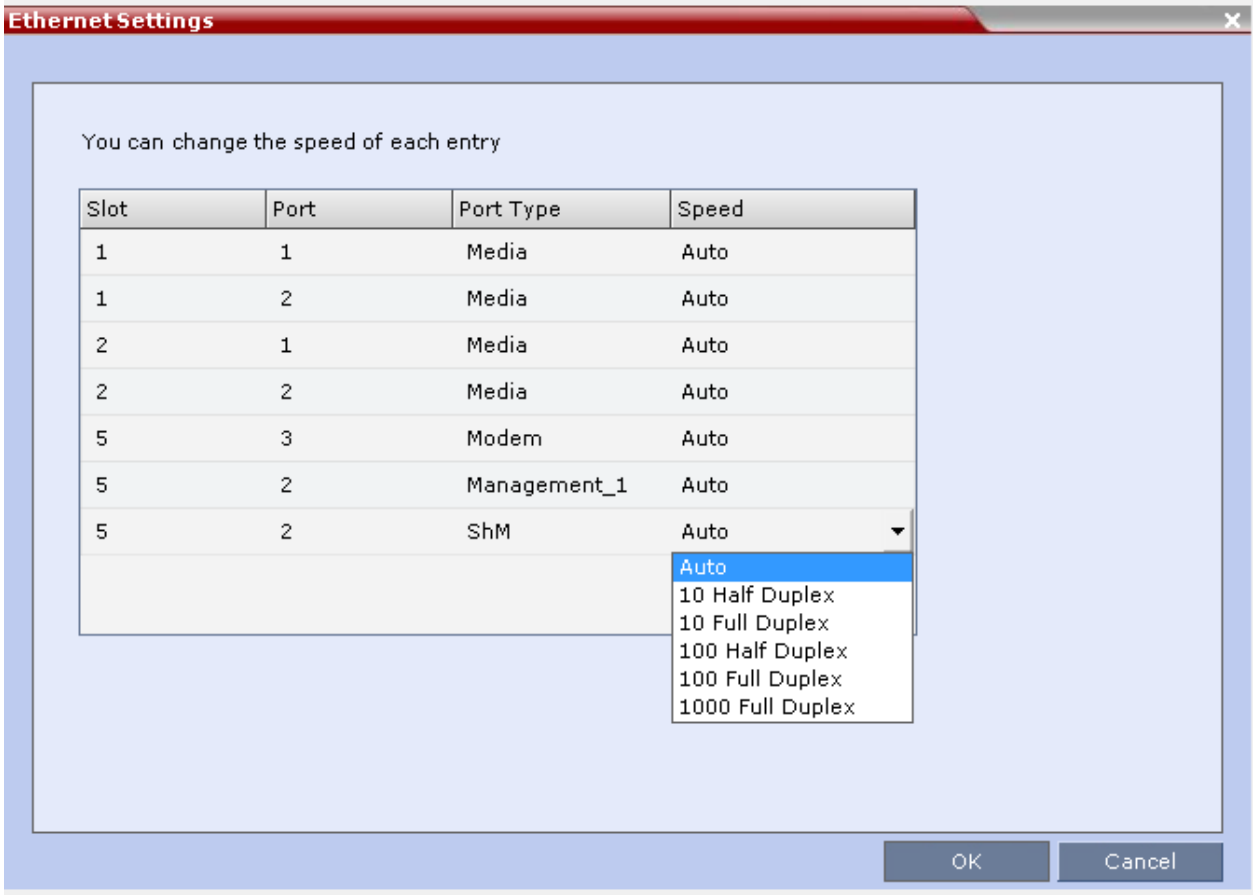
Port Type	*Label on MCU*		
	1500	4000	
Media	LAN 2	LAN 2	RTM LAN Card
Modem	Modem	LAN 1	RTM-IP 4000 Card
Management 1	MNG B	LAN 2	
Signaling 1	MNG	LAN 3	
ShM	Shelf	LAN 6	

To modify the automatic LAN port configuration:

1 On the RMX menu, click **Setup > Ethernet Settings**, shown next.



The Ethernet Settings dialog displays.



Note: The RTM LAN port on the RMX 1500/4000 is Port 2.

Although the RTM LAN (media card) port on the RMX 1500/4000 is shown as Port 1 in the Ethernet Settings and Hardware Monitor fields, the physical LAN connection is Port 2.

2 Modify the following fields:

- **Port Type** Indicates the LAN port type.
- **Speed** Select the speed and transmit/receive mode for each port. Note that the default speed is Auto. When set to Auto, negotiation of speed and transmit and receive mode starts at 1000 Mbps Full Duplex and proceeds downward to 10 Mbps Half Duplex.

Note: Do Not Change Ports 1, 4, and 5 of the Management 2 and Signaling 2 Networks

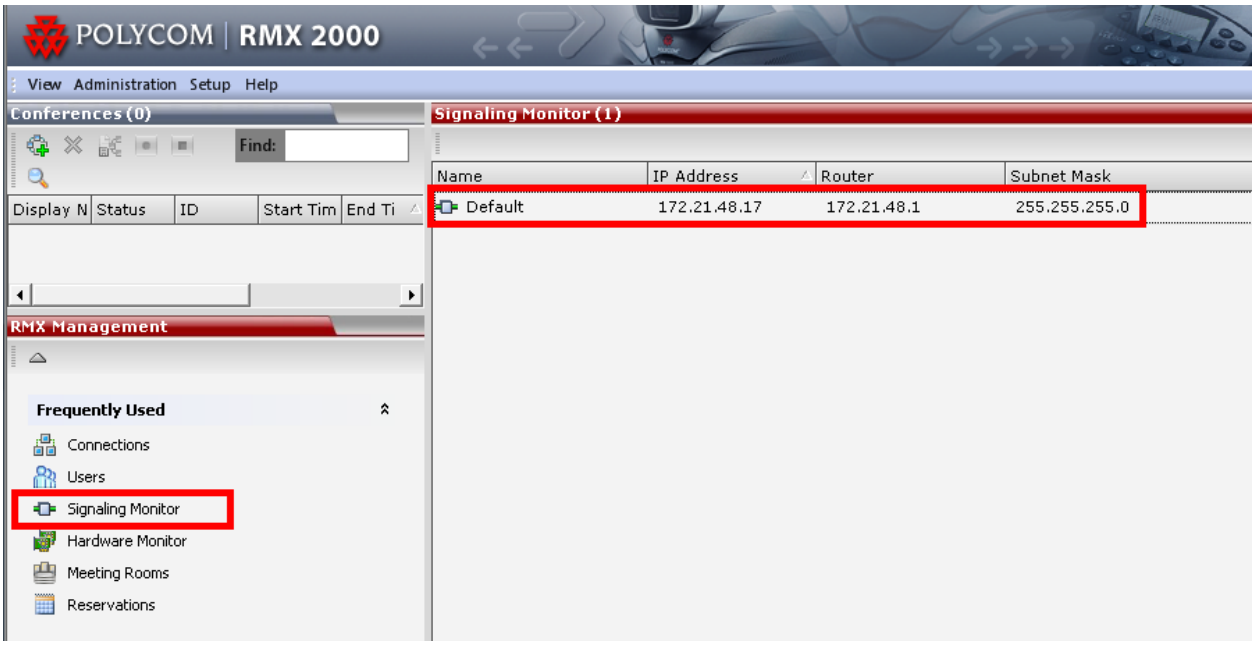
Do not change the automatic setting of Port 1,4 and Port 5 of the Management 2 and Signaling 2 Networks. Any change to the speed of these ports will not be applied.

Monitoring the IP Network

The Signaling Monitor is the RMX entity used to monitor the status of external IP network entities such as the gatekeeper, DNS, SIP proxy, and Outbound proxy and their interaction with the MCU.

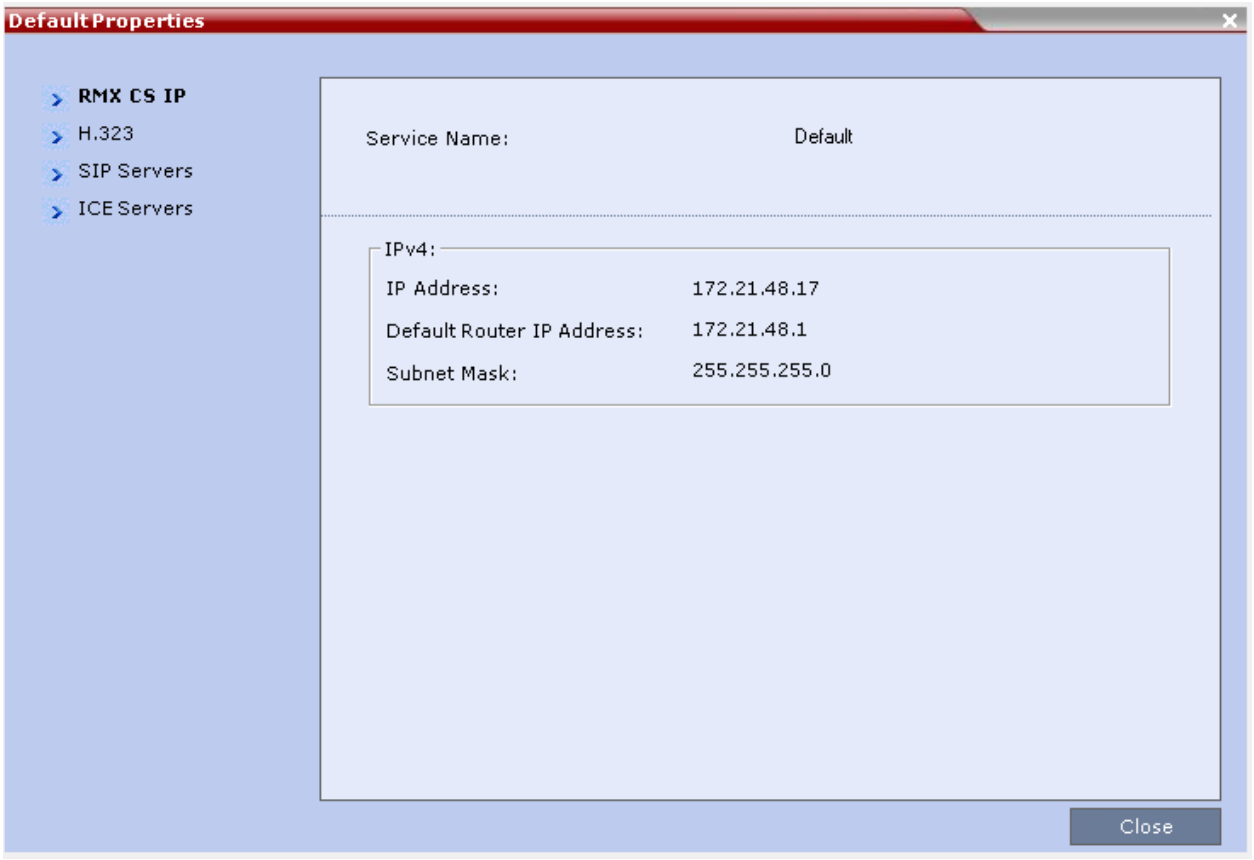
To monitor signaling status:

1 In the RMX Management pane, click **Signaling Monitor**, shown next.



2 In the Signaling Monitor pane, choose the Default IP Service.

The RMX CS IP tab displays.



The RMX CS IP screen displays the following settings:

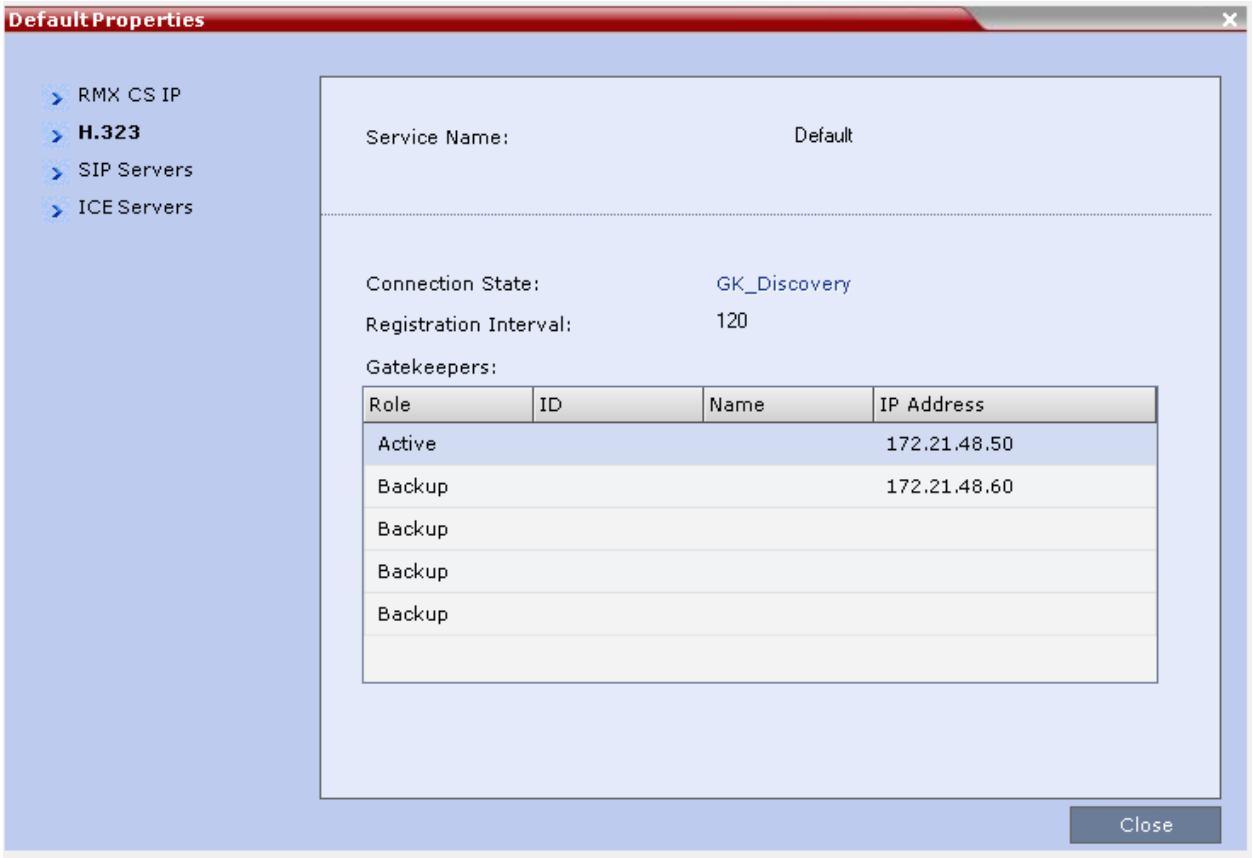
- **Service Name** The name assigned to the IP Network Service by the Fast Configuration Wizard.
- **IPv4**
  - **IP Address** the IP address of the RMX.
  - **Default Router IP Address** The IP address of the default router. The default router is used whenever the defined static routers are unable to route packets to their destination. The default router is also used when host access is restricted to one default router.
  - **Subnet Mask** The subnet mask of the MCU. The default value is 255.255.255.0.

If you have configured IPv6 in network Services, the following IPv6 display:

- **IPv6**
  - **Scope** IP Address
  - **Global** The Global Unicast IP address of the RMX.
  - **Site-Local** The IP address of the RMX system within the local site or organization.
  - **Default Router IP Address** The IP address of the default router. The default router is used whenever the defined static routers are unable to route packets to their destination. The default router is also used when host access is restricted to one default router.

3 Click **H.323**.

The H.323 settings display.



- Connection State The state of the connection between the Signaling Host and the gatekeeper:
  - **Discovery** The Signaling Host is attempting to locate the gatekeeper.
  - **Registration** The Signaling Host is in the process of registering with the gatekeeper.
  - **Registered** The Signaling Host is registered with the gatekeeper.
  - **Not Registered** The registration of the Signaling Host with the gatekeeper failed.
- **Registration Interval** The interval in seconds between the Signaling Host's registration messages to the gatekeeper. This value is taken from either the IP Network Service or from the gatekeeper during registration. The lesser value of the two is chosen.
- **Role**
  - **Active** The active gatekeeper.
  - **Backup** The backup gatekeeper that can be used if the connection to the preferred gatekeeper fails.
- **ID** The gatekeeper ID retrieved from the gatekeeper during the registration process.
- **Name** The gatekeeper's host's name.

- **IP Address** The gatekeeper's IP address.

4 Click **SIP Servers**.

The SIP Servers settings display.

- **Role**
  - » **Active** The default SIP Server is used for SIP traffic.
  - » **Backup** The SIP Server is used for SIP traffic if the preferred proxy fails.
- **Name** The name of the SIP server.
- **IP** The SIP server's IP address.
- **Status** The connection state between the SIP Server and the Signaling Host.
  - » **Not Available** No SIP server is available.
  - » **Auto** Gets information from DHCP, if used.

Using IPv6 Network Addresses for RMX Internal and External Entities

Not all IPv6 settings are available. You can assign the following IPv6 addresses to RMX (Internal) and External Entity addresses.

RMX Internal Addresses

Default Management Network Service

- Control Unit
- Signaling Host
- Shelf Management
- MPM1 (Media Card)
- MPM2 (Media Card)

External Entities

- Gatekeepers (Primary & Secondary)
- SIP Proxies
- DNS Servers
- Default Router
- Defined participants

IPv6 Guidelines

The following is a list of guidelines when using IPv6:

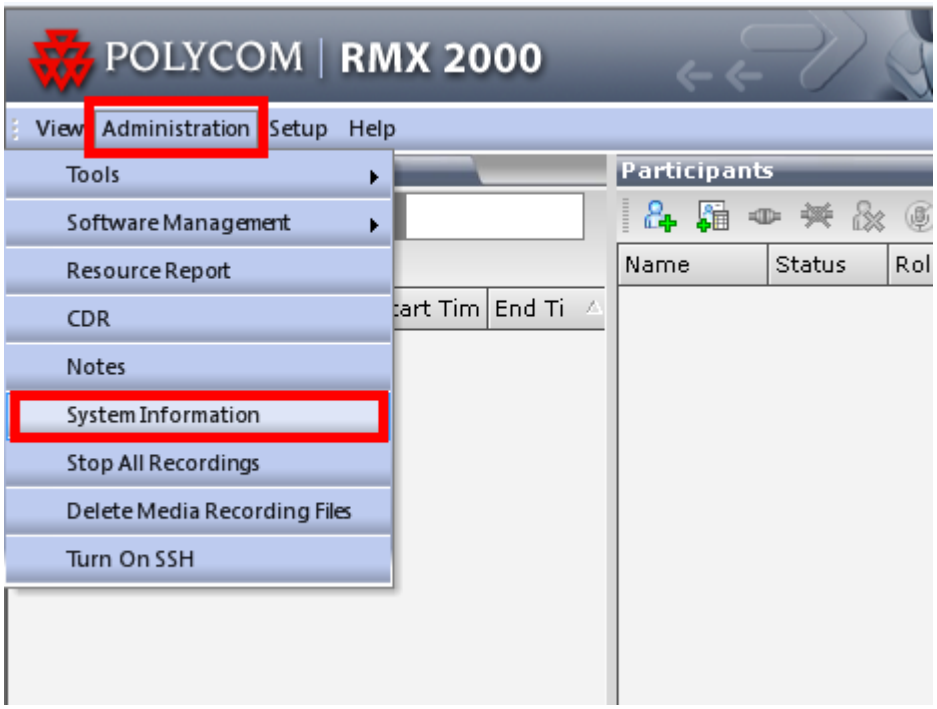
- You must use Internet Explorer 7 to connect the RMX Web Client and RMX Manager to the RMX system using IPv6.
- IPv6 is supported with MPM+ and MPMx media cards only.
- The default IP address version is IPv4.
- You can define the IP address field in the address book entry for a defined participant as either IPv4 or IPv6. You cannot add a participant with an IPv4 address to an ongoing conference while the RMX system is in IPv6 mode nor can you add a participant with an IPv6 address while the RMX system is in IPv4 mode.
- Participants that do not use the same IP address version as the RMX system in ongoing conferences launched from Meeting Rooms, Reservations and Conference Templates are disconnected. An error message, Bad IP address version, is displayed.
- IP Security (IPSec) Protocols are not supported.

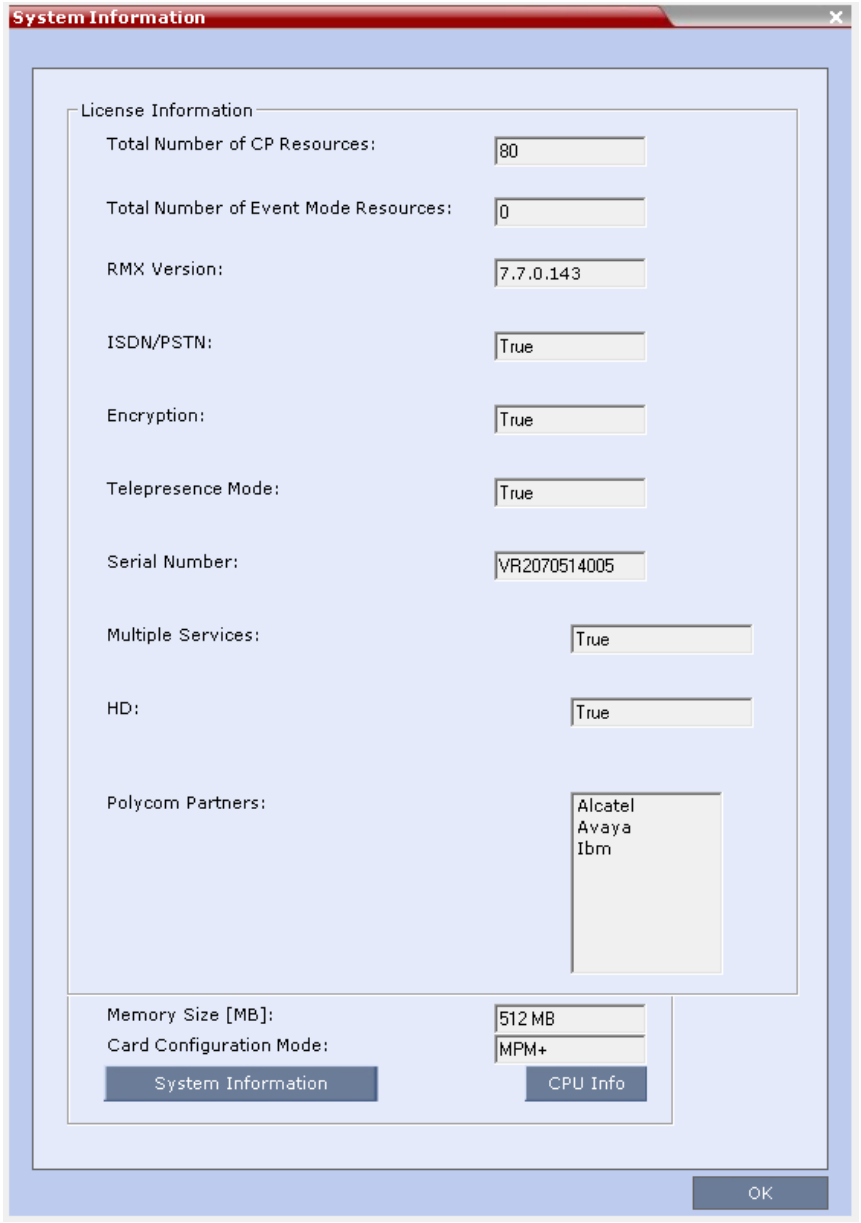
Viewing Licensing and System Information

You can view licensing and system information for your RMX. System Information includes License Information, and general system information, such as system memory size and Media Card Configuration Mode.

To view the System Information properties box:

1 On the RMX menu, click **Administration > System Information**.





The System Information screen displays the following information:

- **Total Number of CP Resources**

  Total Number of Event Mode Resources Note that event mode is currently not supported and this field will always display zero resources.

- **RMX Version** Displays the System Software Version of the RMX.
- **ISDN/PSTN** The field value indicates whether RTM ISDN/ PSTN hardware has been detected in the system. You can choose True or False.
- **Encryption** The field value indicates whether encryption is included in the MCU license. Encryption is not available in all countries. You can choose True or False.

- **Telepresence Mode** The field value indicates whether the system is licensed to work with RPX and TPX Telepresence room systems. You can choose True or False.
- **Serial Number** This field displays the serial number of the RMX system.
- **Multiple Services** A *Multiple Services* license is installed.
- **HD** If you are using the RMX 1500 with a MPMx-Q media card, you will need an additional license if you want to use HD with Continuous Presence.
- **Polycom Partners** The field value indicates that the system software contains features for the support of specific Polycom Partner environments.
- **Memory Size (MB)** This field indicates the RMX system memory size in MBytes. Specify one of the following values:
  - **1024 MB** Version 7.1 requires 1024 Mbytes of memory.
  - **500 MB** If memory size is 512MB, Version 7.1 is not supported.
  - **2048 MB** Specify this memory size when using the RMX 4000.
- **Card Configuration Mode** Indicates the MCU configuration as derived from the installed media cards:
  - **MPM+** Only MPM+ cards are supported. MPMx cards in the system are disabled.
  - **MPMx** Only MPMx cards are supported. MPM+ cards in the system are disabled.

Notes on Card Configuration Mode:

- When you start with Version 7.7 installed, the RMX system enters MPMx mode by default, even if no media cards are installed.
- The RMX system switches between MPM+ and MPMx Card Configuration Modes only if MPM+ or MPMx cards are removed or swapped while the RMX is powered on.
- The Card Configuration Mode switch occurs during the next restart.
- Installing or swapping MPM+ or MPMx cards while the RMX system is off will not cause a mode switch when the system is restarted. The RMX starts in the Card Configuration Mode that was active previous to powering down.

Chapter 8: Integrating Polycom VVX Phones with Siemens OpenScape

This chapter provides an overview of how to set up Polycom® VVX® business media phones for integration with Siemens OpenScape® products. For more detailed information about configuring VVX phones, refer to the documentation on the Polycom Support site.

Polycom VVX phones running Polycom UC Software version 4.0.2 and later can place and receive calls with Siemens OpenScape Desktop Client PE version 6 and OpenScape Desktop Client WE version 6 and with Siemens OpenScape Voice version6.

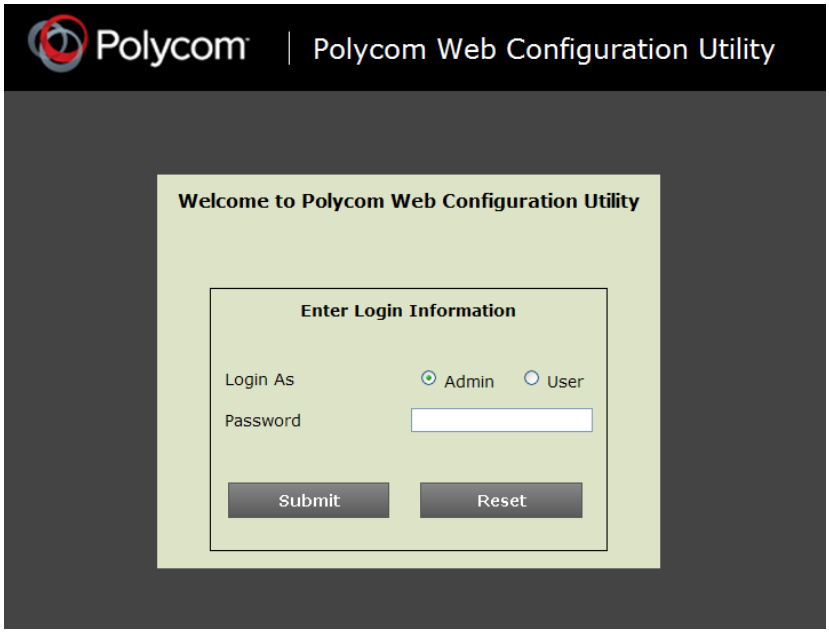
Configuring Polycom VVX 1500 SIP Settings

This section shows you how to configure VVX 1500 phone and SIP system properties for integration with Siemens OpenScape. You can use the Polycom Web Configuration Utility to configure settings for a single VVX 1500 device.

To configure VVX 1500 and SIP properties:

1 Launch your web browser and enter the IP Address of your VVX 1500, for example, `http://10.1.1.24` .

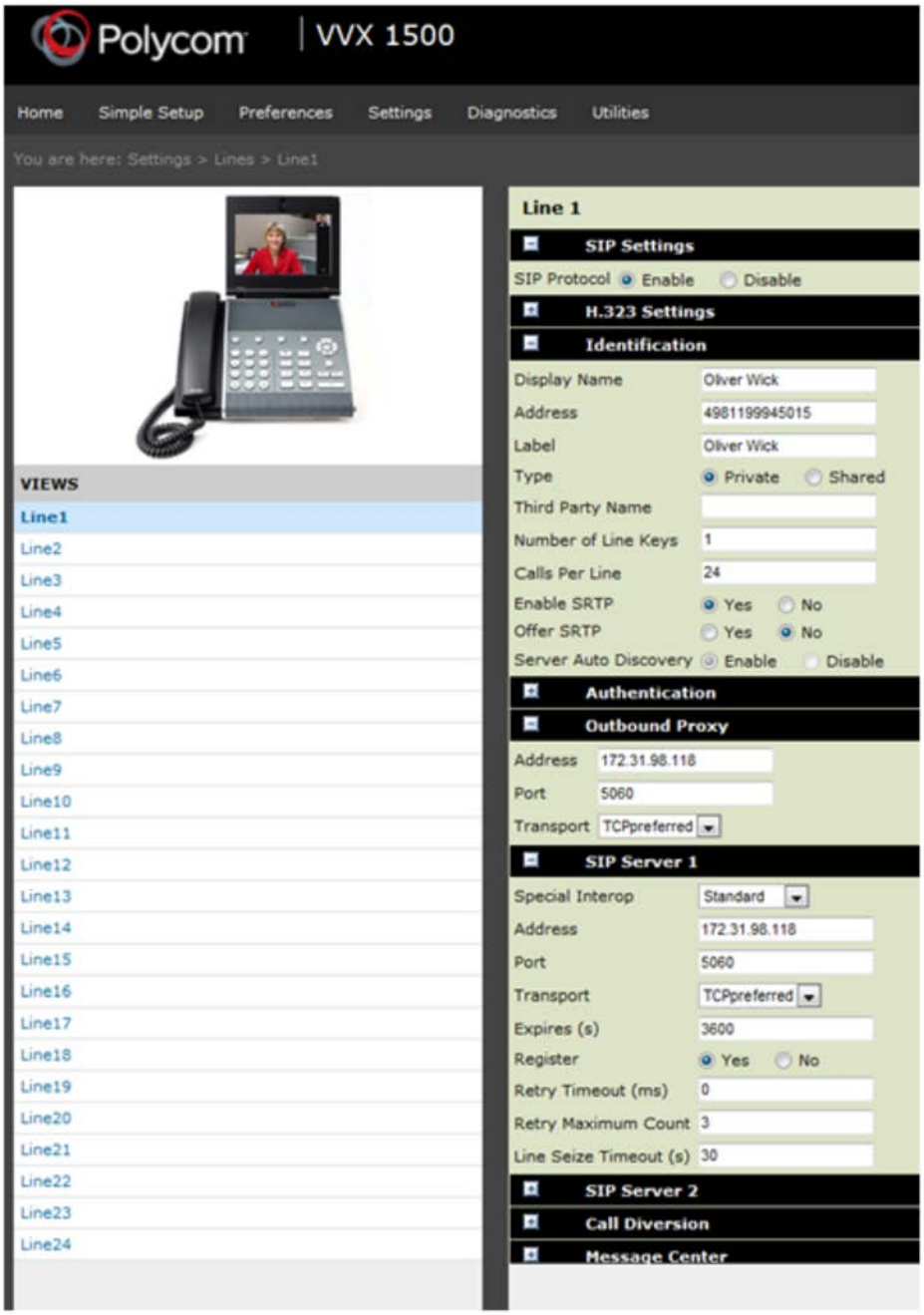
The Web Configuration Utility login screen displays.



2 Choose to log in as **Admin** and enter the **Password** (default 456).

3 Go to **Settings > Lines**, and choose the **Line Key** you want to configure.

The settings for that line display, shown next.



4 Configure the following values:

- **SIP Settings**
  - » **SIP Protocol** Choose Enable
- **Identification**

- » **Display Name** Enter the name of the phone user.
- » **Address** Enter the directory number of the OpenScape Video.
- » **Label** Enter the name you want to display on the line key of another party you call.

○ **Authentication**

- » **Authentication User ID** Enter the digest authentication user name.
- » **Authentication Password** Enter the digest authentication user name.

○ **SIP Server 1**

- » **Address** Enter the OpenScape Video IP or DNS-Name.
- » **Port** 5060
- » **Transport** TCP preferred

Chapter 9: Integrating Polycom DMA Systems with Siemens OpenScape

This chapter provides an overview of how to set up and configure Polycom® Distributed Media Application™ (DMA™) Systems to interoperate with Siemens OpenScape® products. For more detailed information about configuring DMA systems, refer to the documentation on the Polycom Support site.

Polycom DMA systems running software version 5.0 and later can place and receive calls with Siemens OpenScape Desktop Client PE version 6 and OpenScape Desktop Client WE version 6 with Siemens OpenScape Voice version 6.

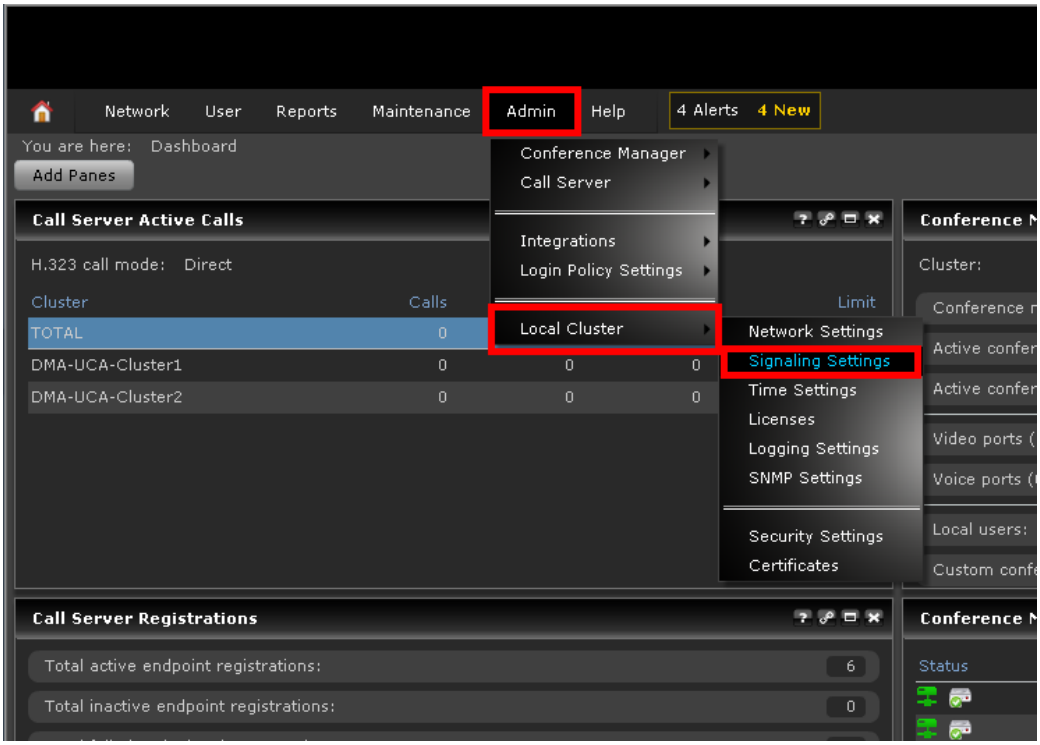
Configuring the Polycom DMA System SIP Settings

This section shows you how to configure the DMA SIP system properties when setting them up to interoperate in a Siemens OpenScape environment.

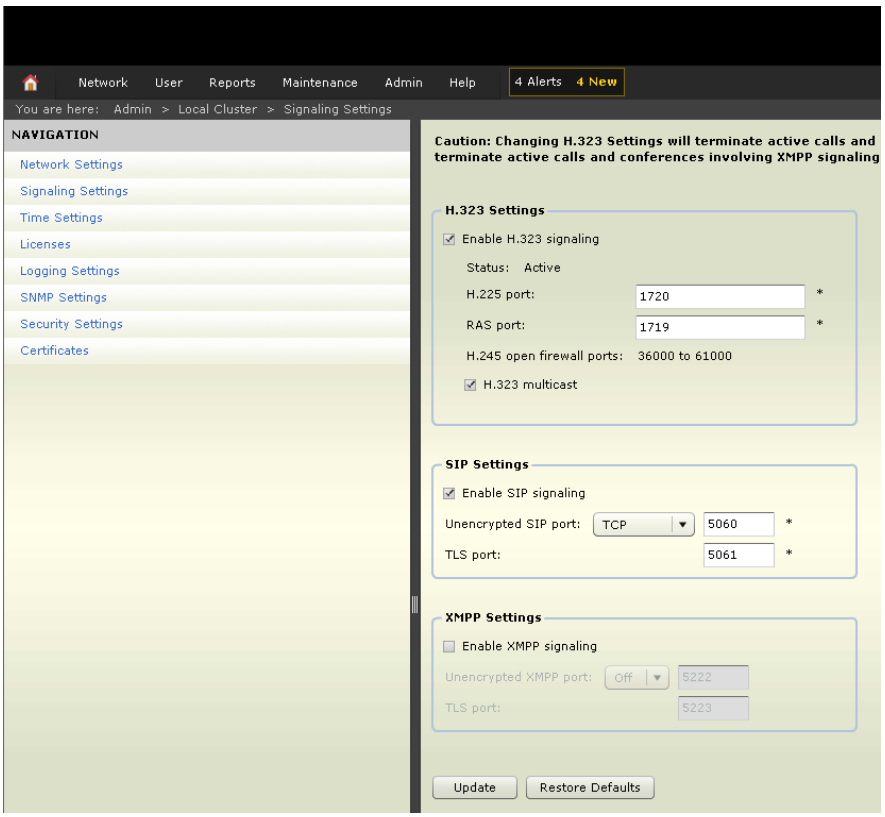
To configure Polycom DMA Signaling Configuration properties:

1. Launch your web browser and enter the IP Address of your DMA System, for example, `http://10.1.1.24` .
2. If your PC's firewall settings cause a security dialog to display, click on **Continue to this website (not recommended)**.
3. Type in the **User ID** (default is admin) and type in the **Password** (default is admin).
4. Select your **Domain** (default is LOCAL).

5 Go to **Log in > Admin > Local Cluster > Signaling Settings**, as shown next.



The DMA Signaling Configuration screen displays.



6 Configure the following settings on the DMA Signaling Configuration screen:

- **SIP Settings**
  - » **SIP Signaling** Check to enable.
  - » **Unencrypted SIP port** Choose TCP, 5060.
  - » **TLS port** 5061

Next, add an external SIP peer.

To external SIP peer the DMA system:

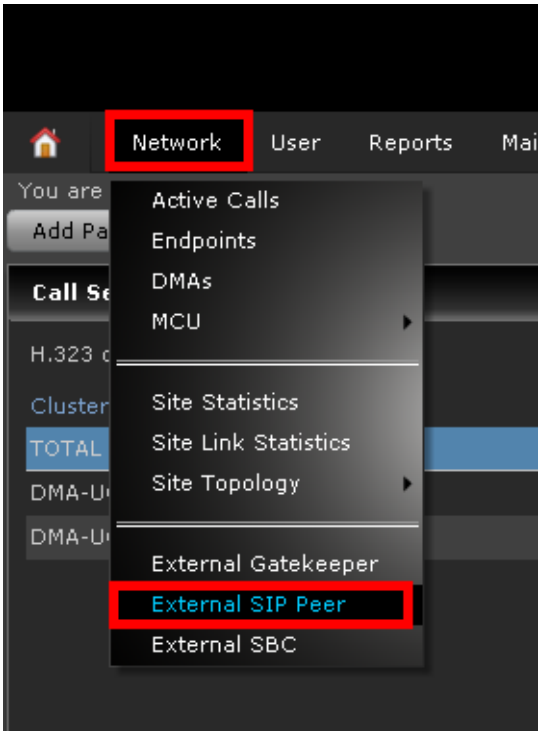
1 Launch your web browser and enter the IP Address of your DMA System, for example, `http://10.1.1.24` .

2 Click on **Continue to this website (not recommended)**.

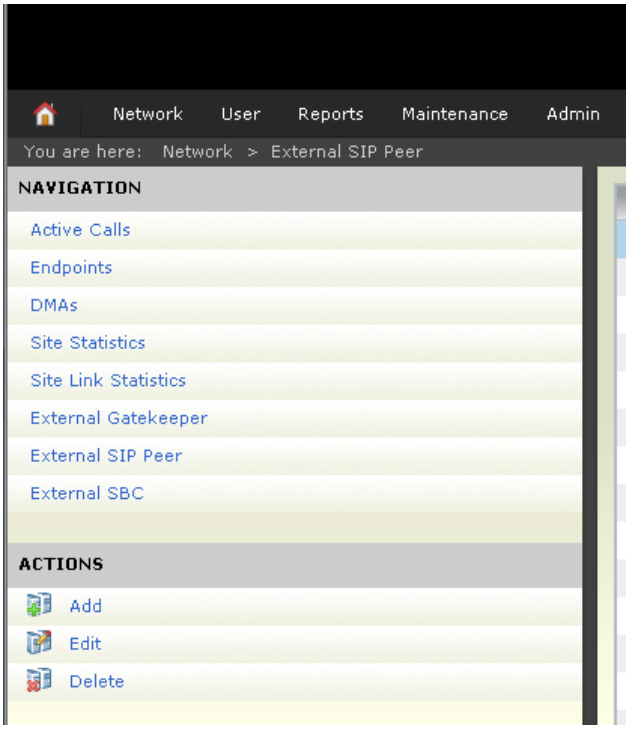
3 Type in the **User ID** (default is admin) and type in the **Password** (default is admin).

4 Select your **Domain** (default is LOCAL).

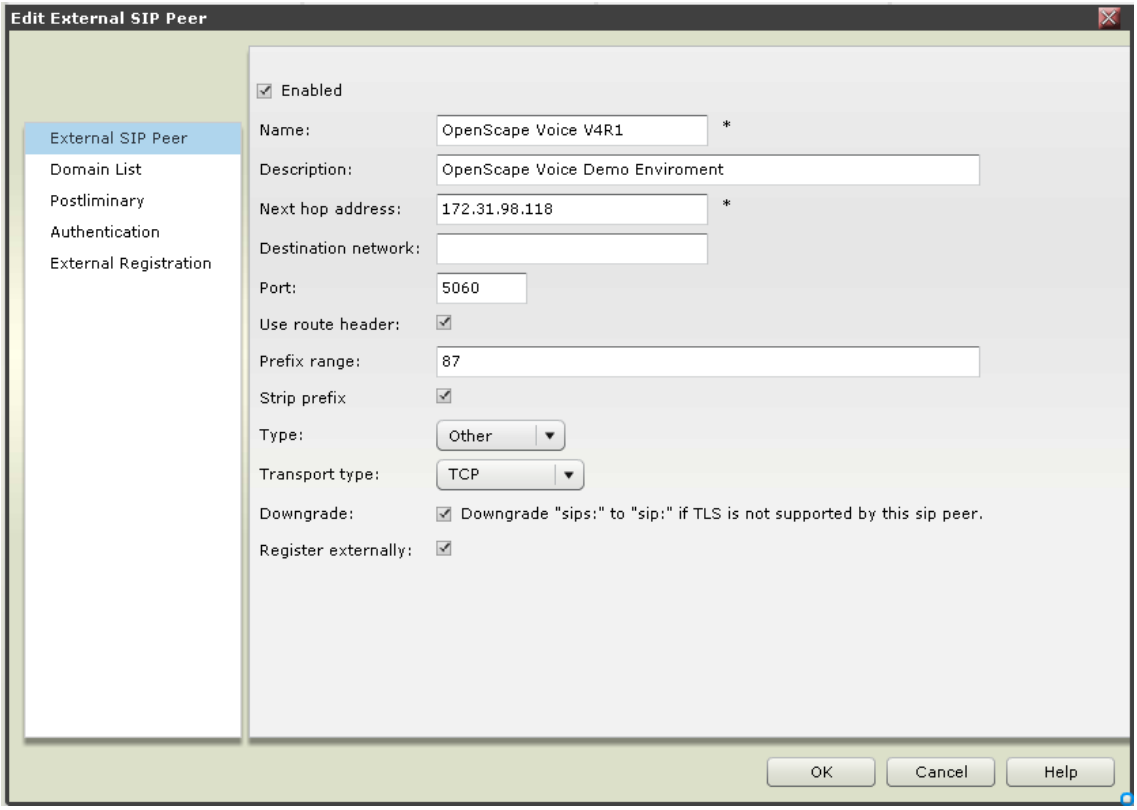
5 Go to **Log in > Network > External SIP Peer**, as shown next.



6 Choose to **Add** to add a new SIP Peer or choose **Edit** to modify an existing SIP Peer.



7 The Edit External SIP Peer dialog displays.



8 Configure the following fields:

- **Enabled** Check this option.
- **Name** Enter a name for the SIP trunk.
- **Description** Enter a detailed description (can also be blank).
- **Next hop address** Enter a SIP IP address or the FQDN of the OpenScape Voice.
- **Destination network** Enter the OpenScape Domain name (can also be blank).
- **Port** 5060 for UDP/TCP or 5061 for TLS
- **Use route header** Check this option.
- **Prefix range** Type in a single prefix number.
- **Strip prefix** Check this option.
- **Type** Choose **Other**.
- **Transport type** Choose TCP or TLS.
- **Downgrade** Check this option.
- **Register externally** Check this option.

Chapter 10: Known Issues

The following table lists known issues for this release. If a workaround is available, it is noted in the table.

Table 10-1: Feature Limitations

Issue ID	*Found in Release*	*Description*	*Workaround*
SI-84	RMX V7.2	If an RMX system is reset while there is an active conference, the conference with its SIP participants is not released.	Reset the RMX system after terminating all active conferences.
SI-97	RMX 7.7	The recording link cannot be configured if the RMX system is set up with network separation.	None
SI-136	VVX 3.3.1 HDX 3.0.3	The VVX 1500 connects to the HDX with asymetric codec negotiation (H.263 sending/H.264 receiving).	None
SI-157	HDX 3.0.3	When touch control is connected to HDX, the HDX sends DTMF inband.	None
SI-162	SSIP 3.3.1	On the IP 7000, you cannot make calls from the missed calls list.	None
SI-165	HDX 3.0.5	HDX disabled BFCP after re-invite when used as preferred device and HDX is set to manual answer.	Use Auto-Answer mode. The 3.0.5 hotfix will be available via Polycom global support to address this issue.
SI-173	VVX 4.0.2B	A TLS problem exists between OpenScape Voice and the VVX 1500.	Use TCP or UDP
SI-192	OpenScape V6R0	The HDX and VVX phones disconnect after being put on hold by OpenStage phones during a secured call.	Use TCP or UDP
SI-195	OpenStage V3	Dial-out calls to a Siemens OpenStage phone from the RMX do not connect if TLS and SRTP are enabled.	Use Dial-in scenario or connect the OpenStage phones via TCP or UDP

Issue ID	*Found in Release*	*Description*	*Workaround*
SI-197	HDX 3.0.5	The HDX clears H.323 calls after 2-5 minutes (HDX/ACME/OpenScape Voice).	H323/SIP GW calls via ACME are currently not supported. Use DMA behind the ACME as H.323 to SIP Gateway.